Pacific Journal of Mathematics

EXPLICIT POLYNOMIAL BOUNDS ON PRIME IDEALS IN POLYNOMIAL RINGS OVER FIELDS

WILLIAM SIMMONS AND HENRY TOWSNER

Volume 306 No. 2 June 2020

PACIFIC JOURNAL OF MATHEMATICS
Vol. 306, No. 2, 2020
https://doi.org/10.2140/pjm.2020.306.721

EXPLICIT POLYNOMIAL BOUNDS ON PRIME IDEALS IN POLYNOMIAL RINGS OVER FIELDS

WILLIAM SIMMONS AND HENRY TOWSNER

Consider an ideal $I \subseteq k[x_1, \ldots, x_n]$ of a polynomial ring over a field with the property that for some b, if $fg \in I$ for f, g of degree $\leq b$, then $f \in I$ or $g \in I$. It is known that if b is sufficiently large, then I is prime. We construct an explicit bound on b, polynomial in the degree of the generators of I (the existence of such a bound was established by Schmidt-Göttsch in 1989). We also give a similar bound for detecting maximal ideals in $k[x_1, \ldots, x_n]$.

1. Introduction

Suppose I is an ideal of a polynomial ring over a field, $I \subseteq k[x_1, \ldots, x_n]$, and whenever $fg \in I$ for f, g of degree $\leq b$, then either $f \in I$ or $g \in I$. When b is sufficiently large, it turns out that I is prime. Schmidt-Göttsch [1989] proved that "sufficiently large" can be taken to be a polynomial in the degree of generators of I (with the degree of this polynomial depending on n). However Schmidt-Göttsch used model-theoretic methods to show this, and did not give any indication of how large the degree of this polynomial is. In this paper we obtain an explicit bound on b, polynomial in the degree of the generators of I. We also give a similar bound for detecting maximal ideals in $k[x_1, \ldots, x_n]$.

Our problem belongs to a thread of algorithmic algebra going back over a century. Drawing on the work of Kronecker, Noether, and others, Hermann published in 1926 a seminal paper entitled "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale" [Hermann 1926] (see [Hermann 1998], "The question of finitely many steps in polynomial ideal theory", for an English translation with commentary). Hermann obtained bounds on calculations in polynomial rings over fields such as witnessing ideal membership and finding bases of syzygies. Other tasks she showed to be algorithmically possible include primary decomposition, intersection, and quotients of ideals.

Partially supported by NSF grant DMS-1600263. We thank Florian Pop, Thomas Preu, and Matthias Aschenbrenner for helpful discussions.
MSC2010: primary 12Y05; secondary 12L10.
Keywords: uniform bounds, prime ideals, maximal ideals, proof mining, Gröbner bases.

Seidenberg [1974] analyzed, extended, and in some cases corrected Hermann's work. He noted (see [1974, p. 311]) that one can decide primality of polynomial ideals over "explicitly given fields" by determining if the ideal is primary and, if so, whether the ideal is equal to its associated prime. Seidenberg gave bounds on some steps of the process but did not analyze the complexity of deciding primality.

Buchberger's method of Gröbner bases (introduced in his thesis [1965]; see Section 3 for basic results) provided strong impetus to the development of computational algebra. While many problems are in principle solvable by the methods of Hermann and Seidenberg, the theory of Gröbner bases has grown substantially and is often more convenient. In particular, much work has been done on the complexity of Gröbner bases. Mayr and Meyer [1982] established doubly exponential worst-case bounds on the complexity of Gröbner bases (as a function of the number of indeterminates). Building on subsequent efforts, Dubé [1990] gave a sharper (but still doubly exponential) bound that we take as a starting point for our analysis in Theorem 3.18.

Gröbner basis methods can be used as building blocks for algorithms that test primality in polynomial rings. Gianni, Trager, and Zacharias [Gianni et al. 1988, pp. 157–158] described an algorithm for deciding primality by, among other things, inductively reducing the number of variables to the univariate case. Eisenbud, Huneke, and Vasconcelos [Eisenbud et al. 1992] gave a method for carrying out primary decomposition of ideals in polynomial rings over perfect fields; one may then follow Seidenberg's observation to decide primality. To our knowledge no one has explicitly analyzed the complexity of these algorithms. However, many of our bounds in Section 3 concern steps of the algorithm from [Gianni et al. 1988] as presented in [Adams and Loustaunau 1994].

Bounds and algorithms are closely related, but existence of one does not necessarily imply existence of the other. If a field k is finite, then our results yield a trivial, albeit inefficient, algorithm for checking whether the ideal generated by a given finite set of polynomials over k is prime: see if there is a counterexample among the finite number of polynomials having degree no greater than our bound. (This process uses the fact that ideal membership is decidable.) Nevertheless, primality cannot be effectively decided for arbitrary fields. To see this, recall that if F is a field, a proper ideal generated by a nonzero polynomial g in $F[x]$ is prime if and only if g is irreducible. However, Fröhlich and Shepherdson [1955] gave explicit examples of fields for which irreducibility is algorithmically undecidable.

Another result related to our problem is Lemma 10 of [Chistov 2008]. There Chistov shows that there is a constant $c \in \mathbb{N}$ such that, given an algebraic variety defined by polynomials in n variables of total degree at most d, irreducible components of the variety are defined by polynomials of total degree at most $d^{2^{cn}}$.

Our main result is as follows:

Theorem 1.1. *There exists a function $b(n,d)$ that is polynomially bounded in d and such that for any field k and proper ideal $I \subseteq k[x_1,\dots,x_n]$ with generators of total degree at most d, if $fg \in I$ implies that either $f \in I$ or $g \in I$ for all f, g of degree less than or equal to $b(n,d)$, then I is prime. Moreover,*

$$b(n,d) \le \max\left\{(2d)^{2^{3n^2+2n}}, (2nd)^{n(n+1)^2 2^{4n+6}}\right\}$$

for all $n, d \ge 1$. If either $d > 1 = n$ or $d = 1$ then the values $b(1,d) = d$ or $b(n,1) = 0$, respectively, suffice to ensure primality.

See Theorems 4.26 and 4.35 for the final steps of the proof. The function $b(n,d)$ is defined in the course of the argument and a more compact bound easily follows (see Corollary 4.36):

Corollary 1.2. *We have $b(n,d) \le (2nd)^{n^3 2^{6n^2}}$ for all $n, d \ge 1$.*

Schmidt-Göttsch [1989] showed that $b(n,d)$ is polynomially bounded in d using ultraproduct methods (as in [van den Dries and Schmidt 1984; Schoutens 2010; Göral 2018]), but did not give any explicit calculation of the bound. Abstract results from proof theory [Kohlenbach 2008; Towsner 2018] suggest that it is possible to extract explicit bounds from proofs that use ultraproducts. The authors demonstrated [Simmons and Towsner 2019] that such methods can be used to extract explicit bounds from ultraproduct proofs in commutative and differential algebra [Harrison-Trainor et al. 2012; van den Dries and Schmidt 1984]. (For instance, in Theorem 2.8 and Lemma 7.7 of [Simmons and Towsner 2019] we gave another bound on $b(n,d)$, but that bound was not polynomial in the degree of the generators.) However, the arguments here, while inspired by Schmidt-Göttsch's approach, were not purely extracted by proof theory; instead we bring in known results using Gröbner bases, etc., where possible and add new arguments to simplify (or clarify) the most complicated parts of Schmidt-Göttsch's argument.

2. Outline of the argument

We briefly describe our strategy. We are interested in *counterexamples to primality*, that is, polynomials $f, g \notin I$ such that $fg \in I$. Our goal is to show that if there are no counterexamples to primality of I having degree $b(n,d)$ or less (we say I is *prime up to* $b(n,d)$), then there are no counterexamples of any degree (i.e., I is prime). The main ingredients are localization of polynomial rings, bounds on Gröbner bases for various auxiliary ideals, and bounds on solutions to systems of linear equations over polynomial rings.

- Relabeling if necessary, choose a maximal set of indeterminates $x_1,\dots,x_r$ that is algebraically independent modulo I. By independence mod I we have $k[x_1,\dots,x_r] \cap I = \{0\}$; by maximality $k[x_1,\dots,x_r,x_j] \cap I \ne \{0\}$ for any $j > r$.

Without loss of generality, we may assume that no $x_i \in I$ (otherwise we solve the problem for smaller n).

- Localize with respect to the variables $x_1, \ldots, x_r$; that is, consider the ideal

$$J = Ik(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$$

generated by I in the ring $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$. The first main task is to show that $k[x_1, \ldots, x_n] \cap J = I$. This step requires induction to prove that there are no counterexamples to primality of I in which one factor belongs to $k[x_1, \ldots, x_r]$. Here we use bounds on Gröbner bases of saturation and quotient ideals.

- The second major task is to show that J is maximal. We introduce a maximal ideal M extending J and prove that $J = M$. This step uses various tools such as the primitive element theorem, flat extensions, and bounds on Gröbner bases for elimination ideals. We also require some complicated inductive arguments on the number of variables $x_{r+1}, \ldots, x_n$. Once we know that J is maximal and hence prime, we conclude that I is prime.

We are principally concerned with the inductive definition of $b(n, d)$ and obtaining a relatively clean estimate rather than precise values of constants and lower-order terms. For this reason (and for readability) our estimate of the bound is somewhat relaxed compared to the actual content of the proofs. By following closely, the interested reader may keep track of such details.

3. Preliminary definitions and results

Throughout the section, k denotes an arbitrary field (except for Theorems 3.7 and 3.8, which require that k have positive characteristic).

We use the following algebraic result to control degrees when going from rational functions to polynomials:

Theorem 3.1 (Gauss' lemma). *Let R be a unique factorization domain (UFD) and let F be the fraction field of R. If $p(x) \in R[x]$ factors as $q_1(x)q_2(x)$ in $F[x]$ such that q_1, q_2 have degrees d_1, d_2 in x, then $p(x)$ factors as $p_1(x)p_2(x)$ in $R[x]$ where the degrees of p_1, p_2 are also d_1, d_2, respectively.*

Proof. See, for example, Corollary 2.2 in [Lang 1965]. □

The following version of a well-known theorem in field theory plays a prominent role in Section 4 when we consider the case of zero-dimensional ideals.

Theorem 3.2 (primitive element theorem). *Let $F \subseteq K$ be a field extension, with F being an infinite field. Let $a, b \in K$ be algebraic of degrees r, s, respectively, over F. Further assume that b is separable over F. Then for all but at most $r(s-1)$ choices of $c \in F$, the linear combination $a + cb$ generates the field $F(a, b)$ over F.*

Proof. See [van der Waerden 1970, p. 139]. Though the bound is clear from the proof, we summarize the argument here because it reappears in the proof of Theorem 4.21. Let $\alpha_1, \dots, \alpha_r$ and $\beta_1, \dots, \beta_s$ be the roots (counting multiplicity) of the minimal polynomials f of a and g of b, respectively, over F. (We work in an extension of K containing the roots.) We may assume that $\alpha_1 = a$ and $\beta_1 = b$. By separability, $\beta_i \neq \beta_j$ for $i \neq j$; the list $\alpha_1, \dots, \alpha_r$ may contain repetition. Consider the $r(s-1)$-many equations $\alpha_i + x\beta_j = a + xb$, where $1 \leq i \leq r$ and $j \neq 1$. Since $\beta_j \neq b$, each equation has at most one solution in F and, except for at most $r(s-1)$ elements, none of the infinitely many remaining elements $c \in F$ satisfies any of the equations.

Let $c \in F$ satisfy none of the equations; we claim that $F(a, b) = F(a + cb)$. Consider the polynomials $g(x)$ and $f((a + cb) - cx)$, both of which belong to $F(a + cb)[x]$ and have a common root b. They have no other root in common: another root β_j of g, with $j \neq 1$, yields an argument $(a + cb) - c\beta_j$ of f that cannot equal α_i for any i lest c satisfy a forbidden equation. It follows that g and $f((a+cb)-cx)$ have a GCD of degree 1 in $F(a+cb)[x]$ (if they were coprime, they could have no common root; if the GCD had degree greater than 1, they would have another common root or g would have a repeated root, contradicting separability). This GCD must be $x - b$, whence $b \in F(a + cb)$ and also $a \in F(a + cb)$. □

3A. ***Bounds on solutions to linear equations in polynomial rings.*** Much of our work is done with Gröbner bases, but it is sometimes convenient to use an older tool from [Hermann 1926].

Theorem 3.3. *Let k be a field and let $N_1, N_2 \in \mathbb{N}$. Consider the system of homogeneous equations $\left\{\sum_{j \leq N_2} f_{ij} X_j = 0\right\}_{i \leq N_1}$, where the coefficients f_{ij} are polynomials in $k[x_1, \dots, x_n]$ of total degree at most d. Then every solution in $(k[x_1, \dots, x_n])^{N_2}$ of the system may be written as a linear combination (over $k[x_1, \dots, x_n]$) of solutions that each have total degree at most $(2N_1 d)^{2^n}$.*

Proof. See Theorem 3.2 of [Aschenbrenner 2004] for this version of the bound; other proofs of the basic result are Theorem 1 of [Seidenberg 1974], and Theorem 2 of [Hermann 1926] for the original. □

Remark 3.4. In [Simmons and Towsner 2019, Theorem 2.5], we call this fact "internal flatness" because it is equivalent to flatness of extensions of polynomial rings by internal polynomial rings in the sense of nonstandard analysis; [Aschenbrenner 2004] refers to such results as "effective flatness".

The preceding theorem generalizes to inhomogeneous equations; here the relationship is with faithfully flat extensions.

Theorem 3.5. *Let k be a field and let $N_1, N_2 \in \mathbb{N}$. Consider the system of equations $\left\{\sum_{j \leq N_2} f_{ij} Y_j = h_i\right\}_{i \leq N_1}$, where the $f_{ij}, h_i \in k[x_1, \dots, x_n]$ have total degree at*

most d. If the system has a solution in $(k[x_1, \dots, x_n])^{N_2}$, then there exists a solution $y = (y_1, \dots, y_{N_2})$ such that each y_j has total degree at most $(2N_1 d)^{2^n}$.

Proof. See Theorem 3.4 of [Aschenbrenner 2004] or p. 92 of [Renschuch 1980] for this bound. Seidenberg [Seidenberg 1974] and Hermann [Hermann 1998] gave earlier proofs but contain some errors (see p. 1, [Aschenbrenner 2004]). □

We also need a version of faithful flatness over the function field $k(x_1, \dots, x_n)$.

Theorem 3.6. *Let k be a field and let $N_1, N_2 \in \mathbb{N}$. Consider the system of equations $\left\{\sum_{j \le N_2} f_{ij} Z_j = h_i\right\}_{i \le N_1}$, where the $f_{ij}, h_i \in k[x_1, \dots, x_n]$ have total degree at most d. If the system has a solution in $(k(x_1, \dots, x_n))^{N_2}$, then there exists a solution $z = (z_1, \dots, z_{N_2}) \in (k(x_1, \dots, x_n))^{N_2}$ such that each z_j may be written as a ratio of polynomials of total degree at most $(2N_1 d)^{2^n}$.*

Proof. Let $\tilde{z} = (\tilde{z}_1, \dots, \tilde{z}_{N_2}) \in (k(x_1, \dots, x_n))^{N_2}$ be a solution to the system. Multiply every equation in the system by the product of all denominators of $\tilde{z}_1, \dots, \tilde{z}_{N_2}$. It follows that there is a solution in $(k[x_1, \dots, x_n])^{N_2+1}$ to the homogeneous system $\left\{\sum_{j \le N_2} f_{ij} \widetilde{Z}_j = h_i \widetilde{Z}\right\}_{i \le N_1}$ such that $\widetilde{Z} \neq 0$. Hence Theorem 3.3 implies that there is a solution in $(k[x_1, \dots, x_n])^{N_2+1}$ with each entry having total degree at most $(2N_1 d)^{2^n}$ and $\widetilde{Z} \neq 0$. Divide each entry by the nonzero value of $\widetilde{Z}$ to obtain the desired solution z to the original system. □

The remaining flatness results require the field k to have characteristic $p > 0$.

Theorem 3.7 (cf. [Schmidt-Göttsch 1989, Lemma 2.11]). *Let $p, m, N_1, N_2 \in \mathbb{N}$, with p prime, and let k be a field of characteristic p. Consider the system of homogeneous equations $\left\{\sum_{j \le N_2} f_{ij} Y_j^{p^m} = 0\right\}_{i \le N_1}$, where the f_{ij} are polynomials in $k[x_1, \dots, x_n]$ of total degree at most B. Then every solution in $(k[x_1, \dots, x_n])^{N_2}$ of the system may be written as a linear combination (over $k[x_1, \dots, x_n]$) of solutions that each have total degree at most $\left(2N_1^2 N_2 \binom{B+n}{n} p^{m(n-1)} B\right)^{2^n}$.*

Proof. Let V_0 be a basis in k of the set of k^{p^m}-linear combinations of the coefficients of all the f_{ij}. Define V_1 to be the set of all power products $\{x_1^{l_1} \cdots x_n^{l_n} \mid 0 \le l_j < p^m\}$. Finally, let $V = \{v_0 v_1 \mid v_0 \in V_0, v_1 \in V_1\}$. Since V_0 is a basis and each variable in an element of V_1 has power less than p^m, it follows that V is linearly independent over $k^{p^m}[x_1^{p^m}, \dots, x_n^{p^m}]$. Each f_{ij} may thus be written uniquely as a sum $\sum_{v \in V} f_{ij,v} v$, where $f_{ij,v} \in k^{p^m}[x_1^{p^m}, \dots, x_n^{p^m}]$.

Substituting for f_{ij} and changing the order of addition, the system

$$\left\{\sum_{j \le N_2} f_{ij} Y_j^{p^m} = 0\right\}_{i \le N_1}$$

becomes

$$\left\{\sum_{v \in V} \left(\sum_{j \le N_2} f_{ij,v} Y_j^{p^m}\right) v = 0\right\}_{i \le N_1}.$$

By linear independence, we may replace this with an equivalent system

$$\left\{\sum_{j \le N_2} f_{ij,v} Y_j^{p^m} = 0\right\}_{v \in V,\, i \le N_1}$$

whose coefficients belong to $k^{p^m}[x_1^{p^m}, \dots, x_n^{p^m}]$. This is a polynomial ring over the field k^{p^m}, so by Theorem 3.3 every solution of $\{\sum_{j\le N_2} f_{ij,v} Z_j = 0\}_{v\in V,\, i\le N_1}$ in $(k^{p^m}[x_1^{p^m}, \dots, x_n^{p^m}])^{N_2}$ is a $k^{p^m}[x_1^{p^m}, \dots, x_n^{p^m}]$-linear combination of solutions having bounded degree. That bound depends on the number of equations in the system and on the total degrees of $f_{ij,v}$ as polynomials in $x_1^{p^m}, \dots, x_n^{p^m}$. The former is $N_1|V|$, where $|V|$ is the cardinality of V. In turn, $|V|$ is the product of the cardinalities $|V_0|$ and $|V_1|$. Lemma 3.10 implies that

$$|V_0| \le N_1 N_2 (\text{the number of monomials in any } f_{ij}) \le N_1 N_2 \tbinom{B+n}{n}.$$

Note that $|V_1| \le p^{mn}$, so $|V| = |V_0||V_1| \le N_1 N_2 \binom{B+n}{n} p^{mn}$. Since the $f_{ij,v}$ are obtained by factoring out powers of $x_1^{p^m}, \dots, x_n^{p^m}$ from monomials of the f_{ij}, the degree of the $f_{ij,v}$ as polynomials in $k^{p^m}[x_1^{p^m}, \dots, x_n^{p^m}]$ is at most $\frac{B}{p^m}$. Thus, by Theorem 3.3, the desired bound is

$$\left(2N_1|V|\tfrac{B}{p^m}\right)^{2^n} \le \left(2N_1^2 N_2 \tbinom{B+n}{n} p^{m(n-1)} B\right)^{2^n}. \qquad \square$$

Theorem 3.8. *Let $p, m, N_1, N_2 \in \mathbb{N}$, with p prime, and let k be a field of characteristic p. Consider the system of equations $\{\sum_{j\le N_2} f_{ij} Y_j^{p^m} = h_i\}_{i\le N_1}$, where f_{ij}, h_i are polynomials in $k[x_1, \dots, x_n]$ of total degree at most B. If the system has a solution in $(k(x_1, \dots, x_n))^{N_2}$, then there is a solution $y = (y_1, \dots, y_{N_2})$ in $(k(x_1, \dots, x_n))^{N_2}$ such that each y_j may be written as a ratio of polynomials of total degree at most*

$$\left(2N_1^2(N_2+1)\tbinom{B+n}{n} p^{m(n-1)} B\right)^{2^n}.$$

Proof. We use the same approach as in Theorem 3.6. Consider the homogeneous system $\{\sum_{j\le N_2} f_{ij} Y_j^{p^m} - h_i Y^{p^m} = 0\}_{i\le N_1}$, where Y is a new indeterminate. By Theorem 3.7, every solution in $(k[x_1, \dots, x_n])^{N_2+1}$ of the homogeneous system is a $k[x_1, \dots, x_n]$-linear combination of solutions that each have total degree at most $\left(2N_1^2(N_2+1)\binom{B+n}{n} p^{m(n-1)} B\right)^{2^n}$. There is a solution in $(k(x_1, \dots, x_n))^{N_2}$ to the original system, so by clearing denominators we obtain a solution in $(k[x_1, \dots, x_n])^{N_2+1}$ to the homogeneous system for which $Y \ne 0$. Therefore there is a bounded solution $\tilde{y} = (\tilde{y}_1, \dots, \tilde{y}_{N_2}, \tilde{y}_{N_2+1}) \in (k[x_1, \dots, x_n])^{N_2+1}$ such that $\tilde{y}_{N_2+1} \ne 0$. Divide $\tilde{y}$ by $\tilde{y}_{N_2+1}$ to obtain a bounded solution $(\tilde{y}_1/\tilde{y}_{N_2+1}, \dots, \tilde{y}_{N_2}/\tilde{y}_{N_2+1}, 1)$ in $(k(x_1, \dots, x_n))^{N_2+1}$. Then $y := (\tilde{y}_1/\tilde{y}_{N_2+1}, \dots, \tilde{y}_{N_2}/\tilde{y}_{N_2+1})$ is the desired solution to the original equation. $\square$

3B. ***Gröbner Bases.*** The basic properties of Gröbner bases are laid out in many places; see, for instance, [Adams and Loustaunau 1994; Buchberger and Winkler 1998; Becker and Weispfenning 1993; Cox et al. 1992; Kreuzer and Robbiano 2000]. We need the following notions and facts.

Definition 3.9. In the polynomial ring $k[x_1, \ldots, x_n]$, a *power product* of variables $x_1, \ldots, x_n$ is a product $x_1^{r_1} \cdots x_n^{r_n}$ for some nonnegative integers r_i (if all r_i are zero, we write 1 for the product). A *monomial ordering* $<$ on $k[x_1, \ldots, x_n]$ is a well-ordering of the set of power products such that

(1) the product 1 is the least element with respect to $<$, and

(2) $<$ respects multiplication by power products: if $x_1^{r_1} \cdots x_n^{r_n} < x_1^{s_1} \cdots x_n^{s_n}$, then

$$\begin{aligned}(x_1^{t_1} \cdots x_n^{t_n})(x_1^{r_1} \cdots x_n^{r_n}) &= x_1^{r_1+t_1} \cdots x_n^{r_n+t_n} \\ &< x_1^{s_1+t_1} \cdots x_n^{s_n+t_n} = (x_1^{t_1} \cdots x_n^{t_n})(x_1^{s_1} \cdots x_n^{s_n}).\end{aligned}$$

Lemma 3.10. *For positive integers n, d, there are $\binom{d+n-1}{n-1}$ power products of total degree d in the indeterminates $x_1, \ldots, x_n$. Counting 1 as a power product with each variable having degree 0, there are $\binom{d+n}{n}$ power products of total degree at most d.*

Proof. This follows from an elementary counting argument; see, e.g., the "stars and bars" method in [Stanley 1986]. □

Definition 3.11. Let $<$ be a monomial ordering on $k[x_1, \ldots, x_n]$. The *leading term* $\mathrm{LT}(f)$ of a nonzero polynomial f is the monomial $ax^{r_1} \cdots x^{r_n}$ of f such that the power product $x^{r_1} \cdots x^{r_n}$ is maximal with respect to $<$. The coefficient a of the leading term is the *leading coefficient* $\mathrm{LC}(f)$ of f. (Note that a monomial is simply a power product multiplied by a field element.)

Definition 3.12. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let $<$ be a monomial ordering on $k[x_1, \ldots, x_n]$. A set of nonzero polynomials $\{g_1, \ldots, g_t\}$ belonging to I is a *Gröbner basis* (with respect to $<$) for I if for every $f \in I$ there exists some i such that the leading term $\mathrm{LT}(g_i)$ of g_i divides the leading term $\mathrm{LT}(f)$ of f.

Definition 3.13. Let $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$ be a finite set of nonzero polynomials. A polynomial $f \in k[x_1, \ldots, x_n]$ is *reducible* with respect to F if f contains a nonzero monomial that is divisible by $\mathrm{LT}(f_i)$ for some $1 \le i \le s$. Otherwise we say that f is *reduced modulo* F. A *reduced Gröbner basis* is one such that each generator is reduced with respect to the set containing all the others.

Theorem 3.14 (division algorithm for $k[x_1, \ldots, x_n]$). *Let $F = \{f_1, \ldots, f_s\}$ be a finite set of nonzero polynomials in $k[x_1, \ldots, x_n]$ and let $<$ be a monomial ordering on $k[x_1, \ldots, x_n]$. For every polynomial f, there exist $u_1, \ldots, u_s, r \in k[x_1, \ldots, x_n]$ such that*

(1) $f = u_1 f_1 + \cdots + u_s f_s + r$,

(2) *r is reduced modulo F,*

(3) $\mathrm{LT}(f) \ge \mathrm{LT}(u_i f_i)$ *for all $1 \le i \le s$, and*

(4) *either r is zero, or f is reduced with respect to F (in which case $u_i = 0$ and $f = r$), or $f \neq r \neq 0$ and $\mathrm{LT}(r) \leq \mathrm{LT}(f)$.*

Proof. See Theorem 1.5.9 of [Adams and Loustaunau 1994]. □

When $f = u_1 f_1 + \cdots + u_s f_s + r$ as in the theorem, we say f *reduces* to r modulo F.

Theorem 3.15. *Let G be a Gröbner basis for a nonzero ideal I. A polynomial $f \in k[x_1, \ldots, x_n]$ belongs to I if and only if f reduces to 0 modulo G.*

Proof. See Theorem 1.6.2 of [Adams and Loustaunau 1994]. □

Definition 3.16. Let $f, g \in k[x_1, \ldots, x_n]$. Let $\mathrm{LCM}(t_1, t_2)$ denote the least common multiple of two power products t_1, t_2. We define the S-polynomial $S(f, g)$ of f, g to be

$$\left(\frac{\mathrm{LCM}(\mathrm{LT}(f), \mathrm{LT}(g))}{\mathrm{LT}(f)}\right) \cdot f - \left(\frac{\mathrm{LCM}(\mathrm{LT}(f), \mathrm{LT}(g))}{\mathrm{LT}(g)}\right) \cdot g.$$

Theorem 3.17 (Buchberger's criterion). *Given a monomial ordering, let G be a finite set of nonzero polynomials in $k[x_1, \ldots, x_n]$. G is a Gröbner basis of the ideal generated by G if and only if $S(f, g)$ reduces to 0 modulo G for all $f, g \in G$.*

Proof. See Theorem 1.7.4 of [Adams and Loustaunau 1994]. □

Theorem 3.18. *Let I be a nonzero ideal of $k[x_1, \ldots, x_n]$ generated by polynomials of total degree at most d. Then for any monomial ordering there is a reduced Gröbner basis of I whose elements have total degree at most*

$$b_1(n, d) := \min\left\{2d^{2^n}, 2\left(\tfrac{1}{2}d^2 + d\right)^{2^{n-1}}\right\}.$$

Proof. The bound $2\left(\frac{1}{2}d^2 + d\right)^{2^{n-1}}$ was given by Dubé [1990, Corollary 8.3]. Note also that $2d^{2^n}$ is greater than or equal to Dubé's bound whenever $d > 1$. For $d = 1$, the constant bound 1 suffices: it follows from Buchberger's criterion (Theorem 3.17) that after Gaussian elimination we are left with a Gröbner basis; see Theorem 5.68 in [Becker and Weispfenning 1993]. □

Remark 3.19. We consider the more generous bound $2d^{2^n}$ because later we compose bounds with each other and we desire a relatively clean final answer.

Theorem 3.20. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal generated by polynomials of total degree at most d. If $G = \{g_1, \ldots, g_t\}$ is a reduced Gröbner basis of I whose elements have degree at most $b_1(n, d)$, then $t \leq (b_1(n, d) + 1)^{n-1}$.*

Proof. Since G is reduced, no leading term of g_i divides a leading term of g_j for $i \neq j$. It suffices to find an upper bound on sets of monomials of total degree at most $b_1(n, d)$ such that no monomial in the set divides another. We induct on the number of variables. The constant value 1 clearly works for $n = 1$. Assume the claim holds for $n - 1$. For any $0 \leq \alpha \leq b_1(n, d)$, consider the set $G_{x_1,\alpha}$ of leading

terms of G such that x_1 appears with degree α. Since no element of $G_{x_1,\alpha}$ divides another, the same is true of the set $G_{x_1,\alpha}/(x_1^\alpha)$ of monomials formed by dividing the elements of $G_{x_1,\alpha}$ by x_1^α. By the inductive hypothesis, $G_{x_1,\alpha}/(x_1^\alpha)$ (and hence $G_{x_1,\alpha}$) has at most $(b_1(n,d)+1)^{n-2}$ elements. G is partitioned into $b_1(n,d)+1$ sets of size at most $(b_1(n,d)+1)^{n-2}$, so G has at most $(b_1(n,d)+1)^{n-1}$ elements, as desired. □

Remark 3.21. As noted earlier, we aim for simplicity rather than sharpness. For a more detailed analysis of the number of generators in a Gröbner basis, see [Robbiano 1991]. The issue is closely related to Dickson's lemma; see [Figueira et al. 2011; León Sánchez and Ovchinnikov 2016] for bounds in that setting.

We now convert the basic bound $b_1(n,d)$ into bounds on the auxiliary ideals that appear in the next section.

Definition 3.22. A monomial ordering $<$ of $k[y_1,\dots,y_m,x_1,\dots,x_n]$ is an *elimination ordering* if every power product in $k[x_1,\dots,x_n]$ (other than 1) is greater than every power product in $k[y_1,\dots,y_m]$. If $I \subseteq k[y_1,\dots,y_m,x_1,\dots,x_n]$ is an ideal, then $I \cap k[y_1,\dots,y_m]$ is an *elimination ideal* that eliminates the x-variables.

Theorem 3.23. *Let $<$ be an elimination ordering of $k[y_1,\dots,y_m,x_1,\dots,x_n]$ such that power products in the x-variables are greater than products in the y-variables. Let G be a Gröbner basis with respect to $<$ of an ideal $I \subseteq k[y_1,\dots,y_m,x_1,\dots,x_n]$ such that the elimination ideal $I \cap k[y_1,\dots,y_m]$ is nonzero. Then $G \cap k[y_1,\dots,y_m]$ is a Gröbner basis of $I \cap k[y_1,\dots,y_m]$.*

Proof. See Theorem 2.3.4 of [Adams and Loustaunau 1994]. □

Theorem 3.24. *Let $<$ be an elimination ordering of $k[y_1,\dots,y_m,x_1,\dots,x_n]$ such that power products in the x-variables are greater than products in the y-variables. Let $I \subseteq k[y_1,\dots,y_m,x_1,\dots,x_n]$ be generated by polynomials of total degree at most d. Also suppose that the elimination ideal $I \cap k[y_1,\dots,y_m]$ is nonzero. Then there is a Gröbner basis (with respect to $<$) of $I \cap k[y_1,\dots,y_m]$ whose elements have total degree at most $b_1(m+n,d)$.*

Proof. By Theorem 3.23, the elimination ideal $I \cap k[y_1,\dots,y_m]$ has a Gröbner basis that is a subset of the Gröbner basis of I given by Theorem 3.18. □

Theorem 3.25. *Let $I \subseteq k[x_1,\dots,x_n]$ be generated by polynomials of total degree at most d and let $u \in k[x_1,\dots,x_n]$ also have total degree at most d. If there exists a nonzero polynomial $p \in k[x_1,\dots,x_r][Y]$ (where Y is a new indeterminate and $r \le n$) such that $p(u) \in I$, then there exists a nonzero polynomial $q \in k[x_1,\dots,x_r][Y]$ of total degree at most $b_1(n+1,d)$ such that $q(u) \in I$.*

Proof. Consider the ideal $\tilde{I} = (I, Y-u) \subseteq k[x_1,\dots,x_n,Y]$. Since $p(u) \in I$, it follows that $p(Y) \in \tilde{I}$. Use an elimination ordering in which power products of

$x_{r+1}, \ldots, x_n$ are greater than power products in $x_1, \ldots, x_r, Y$. Since the elimination ideal $\tilde{I} \cap k[x_1, \ldots, x_r, Y]$ is nonzero, by Theorem 3.24, there is a Gröbner basis of $\tilde{I} \cap k[x_1, \ldots, x_r, Y]$ whose elements have total degree at most $b_1(n+1, d)$. Let q be an element of this Gröbner basis; note that $q(Y) \in \tilde{I}$ implies that $q(u) \in I$. □

3C. *Quotients and Saturations.*

Definition 3.26. Let I and J be ideals of a commutative ring R. The *quotient ideal* of I by J (denoted $I : J$) is defined to be

$$\{f \in R \mid Jf \subseteq I\} = \{f \in R \mid gf \in I \text{ for all } g \in J\}.$$

Theorem 3.27. (1) *Let I and J be ideals of $k[x_1, \ldots, x_n]$ and let w be a new variable. Then $I \cap J = (wI, (1-w)J) \cap k[x_1, \ldots, x_n]$.*

(2) *Let I be an ideal of $k[x_1, \ldots, x_n]$ and let f be a nonzero polynomial. Then the quotient ideal $I : (f)$ is $\frac{1}{f}(I \cap (f))$.*

Proof. See [Adams and Loustaunau 1994, Proposition 2.3.5 and Lemma 2.3.11]. □

Theorem 3.28. *If $I \subseteq k[x_1, \ldots, x_n]$ is a nonzero ideal generated by polynomials of total degree at most d and f is a nonzero polynomial of total degree at most d, then the quotient ideal $I : (f)$ has a Gröbner basis whose elements have total degree at most $b_1(n+1, d+1)$.*

Proof. By properties of a monomial ordering, the leading term of a product is the product of the leading terms. It follows from this and Theorem 3.27(2) that by dividing the elements of a Gröbner basis for $I \cap (f)$ by f, we obtain a Gröbner basis for $I : (f)$. Hence it suffices to give a bound on Gröbner bases of $I \cap (f)$. By Theorem 3.27(1), $I \cap (f) = (wI, (1-w)f) \cap k[x_1, \ldots, x_n]$, where w is a new variable. Use an elimination ordering with w the greatest variable to eliminate w from an ideal generated by polynomials of total degree at most $d+1$. Then Theorems 3.18 and 3.24 imply that $I \cap (f)$ has a Gröbner basis of total degree at most $b_1(n+1, d+1)$. □

Definition 3.29. Let A be a commutative ring with 1. A subset S of A is a *multiplicative set* if $1 \in S, 0 \notin S$, and $xy \in S$ for all $x, y \in S$. If I is an ideal of A, the *saturation* of I by S is the set of all elements $a \in A$ such that for some $s \in S$ we have $sa \in I$. We write $I : S^\infty$ to denote the saturation of I by S. If b is a nonnilpotent element of A, we denote the multiplicative set $\{1, b, b^2, \ldots\}$ by b^∞ and write the saturation as $I : b^\infty$.

Remark 3.30. It is easy to see that $I : S^\infty$ is an ideal containing I. An equivalent characterization is that the saturation is the intersection $(S^{-1}I) \cap A$, where $S^{-1}I$ is the ideal generated by I in the localization $S^{-1}A$.

In Theorem 4.4 we saturate an ideal $I \subseteq k[x_1, \ldots, x_n]$ by the multiplicative set $k[x_i] \setminus \{0\}$. To compute bounds on generators of this saturation we must consider Gröbner bases of polynomials with coefficients from more general rings. The definition of a Gröbner basis is slightly different from the field case to account for the fact that coefficients might be zero-divisors or fail to be units. (Monomial orderings on the set of power products are the same, however. Also, in this paper we only consider the case when the coefficient ring is a Noetherian integral domain.) For the precise definition, see Definition 4.1.13 of [Adams and Loustaunau 1994]. The details are not necessary for our purposes because of the following theorem:

Theorem 3.31. *Let G be a Gröbner basis (in the sense of fields) of an ideal I of $k[y, x_1, \ldots, x_n]$ with respect to an elimination order with the x-variables greater than y. Then G is a Gröbner basis (in the sense of Noetherian integral domains) of I viewed as an ideal of $(k[y])[x_1, \ldots, x_n]$.*

Proof. See Theorem 4.1.18 in [Adams and Loustaunau 1994]. □

Theorem 3.32. *Let R be a Noetherian integral domain, let $g \in R[y_1, \ldots, y_m]$ be a nonzero polynomial, and let I be an ideal of $R[y_1, \ldots, y_m]$. Letting w be a new variable, we have $I : g^\infty = (I, wg - 1) \cap R[y_1, \ldots, y_m]$.*

Proof. See Proposition 4.4.1 in [Adams and Loustaunau 1994]. □

Theorem 3.33. *Let R be a Noetherian integral domain and let $I \subseteq R[y_1, \ldots, y_m]$ be an ideal having a Gröbner basis $G = \{g_1, \ldots, g_t\}$ (in the sense of Noetherian integral domains). Let $g = \mathrm{LC}(g_1)\,\mathrm{LC}(g_2) \cdots \mathrm{LC}(g_t)$ be the product of the leading coefficients of the elements of G. Then $I : (R \setminus \{0\})^\infty = I : g^\infty$.*

Proof. See Proposition 4.4.4 in [Adams and Loustaunau 1994]. □

Theorem 3.34. *If $I \subseteq k[x_1, \ldots, x_n]$ is a nonzero ideal generated by polynomials of total degree at most d, then the saturation $I : (k[x_1] \setminus \{0\})^\infty$ has a Gröbner basis whose elements have total degree at most*

$$b_2(n, d) := b_1(n + 1, (b_1(n, d) + 1)^{n-1} b_1(n, d) + 1).$$

Proof. Choose an elimination ordering having x_1 as least variable. By Theorems 3.18 and 3.20, I has a reduced Gröbner basis $G = \{g_1, \ldots, g_t\}$ with respect to this ordering such that the elements of G have total degree at most $b_1(n, d)$ and $t \leq (b_1(n, d) + 1)^{n-1}$. Now view I as an ideal of $(k[x_1])[x_2, \ldots, x_n])$, the polynomial ring in $n - 1$ variables over $k[x_1]$. By Theorem 3.31 we know that G is still a Gröbner basis in the sense of coefficient rings that are Noetherian integral domains. By Theorem 3.33, $I : (k[x_1] \setminus \{0\})^\infty = I : g^\infty$, where $g = \mathrm{LC}(g_1)\,\mathrm{LC}(g_2) \cdots \mathrm{LC}(g_t)$ is the product of the leading coefficients of the elements of G. Thus the degree of g in x_1 is bounded by $t b_1(n, d)$.

Theorem 3.32 shows that $I : g^\infty = (I, wg-1) \cap (k[x_1])[x_2, \ldots, x_n]$, where w is a new variable. Hence $I : (k[x_1] \setminus \{0\})^\infty = (I, wg-1) \cap k[x_1, x_2, \ldots, x_n]$ and we may view $(I, wg-1)$ as an ideal of $k[x_1, x_2, \ldots, x_n, w]$ generated by polynomials of total degree at most $tb_1(n,d)+1$.

Use an elimination ordering with w the greatest variable to eliminate w from $(I, wg-1)$. By 3.18, 3.24, and the bound on t, the resulting elimination ideal has a Gröbner basis of total degree at most

$$b_1(n+1, tb_1(n,d)+1) \le b_1(n+1, (b_1(n,d)+1)^{n-1}b_1(n,d)+1). \qquad \square$$

Theorem 3.35. $\quad b_2(n,d) \le 2^{n2^{n+3}} d^{n2^{2n+1}}$.

Proof. We get a bound of the desired form through the following chain of inequalities:

$$\begin{aligned} b_2(n,d) &= b_1(n+1, (b_1(n,d)+1)^{n-1}b_1(n,d)+1) \\ &\le 2((b_1(n,d)+1)^{n-1}b_1(n,d)+1)^{2^{n+1}} \le 2((2d^{2^n}+1)^{n-1} \cdot 2d^{2^n}+1)^{2^{n+1}} \\ &\le 2((2^2 d^{2^n})^{n-1} \cdot 2^2 d^{2^n})^{2^{n+1}} = 2(2^{2n} d^{n2^n})^{2^{n+1}} \le 2^{n2^{n+3}} d^{n2^{2n+1}}. \end{aligned}$$ $\square$

4. Proof of the main theorem

We continue to use k to denote an arbitrary field. I denotes a proper ideal generated by polynomials $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ of total degree at most d. As explained in the outline, we choose a maximal set of indeterminates that are algebraically independent modulo I. Relabeling if necessary, we may assume they are $x_1, \ldots, x_r$. Since 0 is the only polynomial in $k[x_1, \ldots, x_r] \cap I$, whenever $fg \in I$ for $f \in k[x_1, \ldots, x_r] \setminus \{0\}$, either $g \in I$ or f, g are counterexamples to primality of I.

Definition 4.1. If $I \subseteq k[x_1, \ldots, x_n]$ is a proper ideal and b is a natural number, we say that I is *prime up to b* if for all $f, g \in k[x_1, \ldots, x_n]$ of total degree at most b such that $fg \in I$, either $f \in I$ or $g \in I$. By *maximal up to b*, we mean that for every $f \notin I$ with degree $\le b$, f has an inverse mod I: there is some g with $fg - 1 \in I$.

Before proceeding, we take care of the simple cases in the main theorem:

Theorem 4.2. *Let $I \subseteq k[x_1, \ldots, x_n]$ be a proper ideal generated by polynomials of degree at most d. Let $\{x_1, \ldots, x_r\}$ be a maximal subset of $\{x_1, \ldots, x_r, \ldots, x_n\}$ that is algebraically independent modulo I.*

- *If $n = 1$, then I is prime if I is prime up to d.*
- *If $d = 1$ (with n arbitrary), then I is prime.*
- *If $r = 0$, then I is prime if I is prime up to $nb_1(n,d)$.*
- *If $r = n$, then $I = \{0\}$ and is prime.*

Proof. First let $n = 1$. The ring $k[x_1]$ is a principal ideal domain and I is of the form (f), where f is the greatest common divisor of the given generators of I. Then f has degree at most d and I is prime if and only if f is irreducible (if f is reducible, no proper factor belongs to I). If I is prime up to d, then f is irreducible.

When $d = 1$, then I is generated by linear polynomials, and I is necessarily prime; this follows geometrically from the irreducibility of affine linear varieties. Therefore primality up to any natural number (e.g., 0) vacuously guarantees primality if $d = 1$.

If $r = 0$, by Theorem 3.24 there is a nonzero polynomial $\alpha_i(x_i) \in I \cap k[x_i]$ of degree at most $b_1(n, d)$ for each $x_1, \ldots, x_n$. Using α_i to reduce higher powers of x_i mod I, we see that any f is equivalent mod I to some $\tilde{f}$ of total degree at most $nb_1(n, d)$. Hence $fg \in I$ if and only if $\tilde{f}\tilde{g} \in I$ and then primality up to $nb_1(n, d)$ ensures primality.

The final claim is clear. □

Remark 4.3. If any $x_i \in I$, then modulo I we may assume that x_i does not appear in any polynomials we consider. Our claimed bound on detecting prime ideals increases with n, so having fewer variables only makes the bound easier to prove.

Due to the preceding theorem and remark, we may safely assume in the following work that $n, d > 1$, $0 < r < n$ and that $x_i \notin I$ for any $1 \leq i \leq n$.

Denote by J the ideal generated by I in $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$. The key properties of J are that if I is prime up to a sufficient level, then $I = J \cap k[x_1, \ldots, x_n]$ and J is maximal. Together these prove that I is prime.

4A. *Proof of $I = J \cap k[x_1, \ldots, x_n]$.* To obtain this result we rely heavily on the bounds from Section 3 on Gröbner bases for various kinds of ideals.

Theorem 4.4. *Let $1 \leq i \leq n$. Suppose that $f \in k[x_i]$ is irreducible and that there exists $g \in k[x_1, \ldots, x_n]$ such that $fg \in I$ but $g \notin I$. Then the degree of f is at most*

$$b_3(n, d) := b_1(n + 1, b_2(n, d) + 1).$$

Proof. Let $q_1, \ldots, q_N$ be generators of the saturation ideal

$$I : (k[x_i] \setminus \{0\})^\infty \subseteq k[x_1, \ldots, x_n].$$

By Theorem 3.34, the total degree of each generator is at most $b_2(n, d)$. For each $1 \leq l \leq N$, consider the ideal $(I : (q_l)) \cap k[x_i]$. Since $k[x_i]$ is a PID, each ideal $(I : (q_l)) \cap k[x_i]$ is generated by some polynomial $u_l \in k[x_i]$; in particular, $u_l q_l \in I$. By Theorems 3.28 and 3.24, the degree of u_l is at most $b_3(n, d) := b_1(n + 1, b_2(n, d) + 1)$. Let $f \in k[x_i]$ be irreducible and let g be an element of $k[x_1, \ldots, x_n] \setminus I$ with the property that $fg \in I$. We claim that

$$\deg(f) \leq \max_{1 \leq l \leq N} \{\deg(u_l)\} \leq b_3(n, d).$$

Note that $g \in I : (k[x_i] \setminus \{0\})^\infty$ and so there are $\alpha_l \in k[x_1, \ldots, x_n]$ such that $g = \sum_{l=1}^N \alpha_l q_l$. Multiplying both sides by $\prod_{l=1}^N u_l$, we obtain

$$\big(\textstyle\prod_{l=1}^N u_l\big)g = \big(\prod_{l=1}^N u_l\big)\big(\sum_{l=1}^N \alpha_l q_l\big) = \sum_{l=1}^N \big(\prod_{l=1}^N u_l\big)\alpha_l q_l \in I,$$

so $\prod_{l=1}^N u_l \in (I : (g)) \cap k[x_i]$. Also note that $f \in (I : (g)) \cap k[x_i]$ and that $(I : (g)) \cap k[x_i]$ is proper since $g \notin I$. Given that f belongs to the same proper ideal of $k[x_i]$ as $\prod_{l=1}^N u_l$ and is irreducible, f must generate the ideal and hence divide u_l for some l. In particular, the degree of f is at most the maximum of the degrees of the u_l and is less than or equal to $b_3(n, d)$ as claimed. □

Remark 4.5. Note that the result holds for any variable x_i, not necessarily one of the $x_1, \ldots, x_r$. Also, the proof goes through unchanged for any field L and any ideal of $L[x_1, \ldots, x_n]$ generated by elements of degree at most d. This is important because in Theorem 4.8 we apply Theorem 4.4 after changing the field from k to $k(x_{i_1}, \ldots, x_{i_l})$ for some subset $\{x_{i_1}, \ldots, x_{i_l}\}$ of the variables.

Theorem 4.6. $b_3(n, d) \le 2^{n2^{2n+6}} d^{n2^{3n+2}}$.

Proof. We compute as follows:

$$\begin{aligned} b_3(n, d) &= b_1(n+1, b_2(n, d)+1) \le 2\big(2^{n2^{n+3}} d^{n2^{2n+1}} + 1\big)^{2^{n+1}} \\ &\le 2\big(2^{n2^{n+4}} d^{n2^{2n+1}}\big)^{2^{n+1}} = 2\big(2^{n2^{2n+5}} d^{n2^{3n+2}}\big) \le 2^{n2^{2n+6}} d^{n2^{3n+2}}. \end{aligned}$$ □

We aim to show that $J \cap k[x_1, \ldots, x_n] = I$. We consider arbitrary subsets $\{x_{i_1}, \ldots, x_{i_l}\} \subseteq \{x_1, \ldots, x_r\}$ of cardinality l having certain properties and show inductively that $\{x_{i_1}, \ldots, x_{i_l}, x_{i_{l+1}}\}$ retains the properties. Let

$$\begin{aligned} J_l &:= Ik(x_{i_1}, \ldots, x_{i_l})[\text{remaining variables from } x_1, \ldots, x_n], \\ J_{l+1} &:= Ik(x_{i_1}, \ldots, x_{i_l}, x_{i_{l+1}})[\text{remaining variables from } x_1, \ldots, x_n]. \end{aligned}$$

With this notation we have $J = J_r$.

Theorem 4.7. *Let $1 \le l \le r$ and suppose that $I : (f) = I$ for all irreducible $f \in k[x_{i_1}, \ldots, x_{i_l}]$ and every subset $\{x_{i_1}, \ldots, x_{i_l}\} \subseteq \{x_1, \ldots, x_r\}$ of cardinality l. Then*

(1) *$I : (f) = I$ for all $f \in k[x_{i_1}, \ldots, x_{i_l}] \setminus \{0\}$ (irreducible or not) and*

(2) *$J_l \cap k[x_1, \ldots, x_n] = I$.*

Proof. The reverse containment is trivial for both parts. For the forward direction, let f factor as $\prod_{l=1}^N p_l$ for some irreducible polynomials $p_l \in k[x_{i_1}, \ldots, x_{i_l}]$ and suppose $fg \in I$. It follows that $\big(\prod_{l=2}^N p_l\big)g \in I : (p_1)$, which is equal to I by the hypothesis since p_1 is irreducible. Continuing this way, we conclude that $g \in I$. This proves (1).

For the second claim, let $g \in J_l \cap k[x_1, \ldots, x_n]$. Clearing denominators, we see that $fg \in I$ for some $f \in k[x_{i_1}, \ldots, x_{i_l}]$. Part (1) implies that $g \in I$. □

Theorem 4.8. *Let $1 \leq l < r$ and $n > 1$. Suppose $J_l \cap k[x_1, \ldots, x_n] = I$ for all $\{x_{i_1}, \ldots, x_{i_l}\} \subseteq \{x_1, \ldots, x_r\}$ and $I : (f) = I$ for all irreducible $f \in k[x_{i_1}, \ldots, x_{i_l}, x_{i_{l+1}}]$ of total degree at most $(n-1) \cdot b_3(n, d)$. Then $J_{l+1} \cap k[x_1, \ldots, x_n] = I$.*

Proof. By Theorem 4.7, it suffices to show that $I : (f) = I$ for all irreducible $f \in k[x_{i_1}, \ldots, x_{i_l}, x_{i_{l+1}}]$. Pick any such f. By hypothesis we already have $I : (f) = I$ if the total degree of f is less than or equal to $(n-1) \cdot b_3(n, d)$, so suppose that the degree of f exceeds this. At least one of the $l + 1 \leq r \leq n - 1$ variables must appear with degree greater than $b_3(n, d)$. Without loss of generality we may assume that variable is $x_{i_{l+1}}$ (because we assume the properties in the statement for arbitrary subsets of $\{x_1, \ldots, x_r\}$ of size l). By Gauss' lemma, f remains irreducible over $k(x_{i_1}, \ldots, x_{i_l})$. Since Theorem 4.4 applies to irreducible univariate polynomials over any field and the $x_{i_{l+1}}$-degree of f is greater than $b_3(n, d)$, we deduce that $J_l : (f) = J_l$. Let $g \in k[x_1, \ldots, x_n]$ be such that $fg \in I$. We conclude from $J_l : (f) = J_l$ that $g \in J_l$. It follows that $g \in I$ because by hypothesis $J_l \cap k[x_1, \ldots, x_n] = I$. This proves that $I : (f) = I$ as required. □

Theorem 4.9. *Let $n, d > 1$. If I is prime up to*

$$b_4(n, d) := b_1(n + 1, (n - 1) \cdot b_3(n, d) + 1),$$

then for all $1 \leq l \leq r$, subsets $\{x_{i_1}, \ldots, x_{i_l}\} \subseteq \{x_1, \ldots, x_r\}$, and irreducible polynomials $f \in k[x_{i_1}, \ldots, x_{i_l}]$ of total degree at most $(n-1) \cdot b_3(n, d)$, we have $I : (f) = I$.

Proof. It suffices for the generators of $I : (f)$ to belong to I. By Theorem 3.28, such a generator g has total degree at most $b_4(n, d) := b_1(n + 1, (n - 1) \cdot b_3(n, d) + 1)$. Since $fg \in I$ but $f \notin I$, by primality up to $b_4(n, d)$ we conclude that $g \in I$. □

Theorem 4.10. *Let $n, d > 1$. If I is prime up to $b_4(n, d)$, then $J \cap k[x_1, \ldots, x_n] = I$.*

Proof. We induct on the size l of subsets $\{x_{i_1}, \ldots, x_{i_l}\}$ of $\{x_1, \ldots, x_r\}$ to prove that $J_l \cap k[x_1, \ldots, x_n] = I$ for each $1 \leq l \leq r$. By Theorem 4.9, $I : (f) = I$ for all irreducible $f \in k[x_{i_1}, \ldots, x_{i_l}]$ of total degree at most $(n-1) \cdot b_3(n, d)$. (This satisfies one of the two hypotheses of Theorem 4.8.) Letting $l = 1$, Theorem 4.4 now implies that $I : (f) = I$ for irreducible $f \in k[x_{i_l}]$ of any degree. Theorem 4.7 then yields the base case $J_1 \cap k[x_1, \ldots, x_n]$. We can now apply Theorem 4.8 repeatedly to obtain $J \cap k[x_1, \ldots, x_n] = I$. □

4B. *J is maximal.* We start with an important lemma that allows us to control the degrees of $x_{r+1}, \ldots, x_n$ modulo I.

Lemma 4.11. *Let I be defined as before and suppose I is prime up to $b_1(n, d)$.*

(1) *For each* $r+1 \le j \le n$, *there is a polynomial* $w_j \in I \cap k[x_1, \ldots, x_r][x_j]$ *such that* w_j *has total degree at most* $b_1(n,d)$, *is irreducible, and remains irreducible over* $k(x_1, \ldots, x_r)[x_j]$.

(2) *The* $k(x_1, \ldots, x_r)$*-vector space* $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/J$ *is finite dimensional of dimension at most* $\prod_{j=r+1}^{n} d_j \le (b_1(n,d))^{n-r}$, *where* d_j *is the* x_j*-degree of* w_j *in the first part of the lemma.*

Proof. By definition of $\{x_1, \ldots, x_r\}$ as a maximal algebraically independent set mod I, we know that $I \cap k[x_1, \ldots, x_r] = \{0\}$ and for all $j > r$ there exist elements of positive x_j-degree in $I \cap k[x_1, \ldots, x_r][x_j]$. By Theorem 3.24, $I \cap k[x_1, \ldots, x_r][x_j]$ has a Gröbner basis whose elements have total degree at most $b_1(n,d)$; the x_j-degree of each generator is positive. Consider the set

$$W = \{w \in I \cap k[x_1, \ldots, x_r][x_j] \mid \text{the total degree of } w \text{ is at most } b_1(n,d)\}$$

and let N be the minimal x_j-degree of any element of W. Let $W_N \subseteq W$ be the subset of W whose elements have x_j-degree N. Choose $w_j = a_N x_j^N + \cdots + a_0 \in W_N$ such that $a_N \in k[x_1, \ldots, x_r]$ has minimal total degree out of all coefficients of x_j^N in W_N.

We claim that w_j is irreducible in $k[x_1, \ldots, x_r][x_j]$. To see this, suppose toward contradiction that w_j properly factors as $fg = (b_l x_j^l + \cdots + b_0)(c_m x_j^m + \cdots + c_0)$. Then either $b_l \in k[x_1, \ldots, x_r]$ would have lower total degree than a_N or $l < N$, and likewise for c_m and m. Since f, g have total degree at most $b_1(n,d)$, by primality up to $b_1(n,d)$ we have $f \in I$ or $g \in I$. But this contradicts either minimality of N or that of a_N, so w_j does not factor in $k[x_1, \ldots, x_r][x_j]$. By Gauss' lemma (see Theorem 3.1), w_j remains irreducible over $k(x_1, \ldots, x_r)[x_j]$.

The final claim follows from the existence of the w_j and the definition of d_j. □

Lemma 4.12. *J is contained in a maximal ideal M of $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$.*

Proof. We need only show that J is proper. Suppose on the contrary that 1 is a $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$-linear combination of $f_1, \ldots, f_s$. Then by clearing denominators in an equation witnessing that $1 \in J$, we obtain a nonzero element $k[x_1, \ldots, x_r] \cap I$. This contradicts algebraic independence of $x_1, \ldots, x_r$ mod I. □

We prove that J is maximal by showing that $J = M$. A crucial step is the following:

Proof that elements of M having small degree belong to J. When working in the ring $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$, we must keep track of the variables $x_1, \ldots, x_r$ as well as $x_{r+1}, \ldots, x_n$. For convenience we use the following terminology:

Definition 4.13. Let $\alpha/\beta \in k(x_1, \ldots, x_r) \setminus \{0\}$ with α, β coprime as polynomials in $k[x_1, \ldots, x_r]$. We say the $(x_1, \ldots, x_r)$*-degree* (or just degree) of α/β is the maximum of the total degrees of α and β. A monomial $(\alpha/\beta)T$, where T is a power product in $x_{r+1}, \ldots, x_n$, is defined to have $(x_1, \ldots, x_r)$-degree equal

to the sum of the $(x_1, \dots, x_r)$-degree of α/β and the total degree of T. Given $f \in k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n] \setminus \{0\}$, we define the $(x_1, \dots, x_r)$-degree of f to be the maximum of the $(x_1, \dots, x_r)$-degrees of the monomials appearing in f.

Let $\mathcal{J} \subseteq k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$ be a proper ideal and B a natural number. We say $\mathcal{J}$ is $(x_1, \dots, x_r)$-*prime* up to B if for all $f, g \in k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$ of $(x_1, \dots, x_r)$-degree at most B such that $fg \in \mathcal{J}$, either $f \in \mathcal{J}$ or $g \in \mathcal{J}$. Likewise, if every $f \in k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n] \setminus \mathcal{J}$ of $(x_1, \dots, x_r)$-degree at most B is invertible mod $\mathcal{J}$, we say that $\mathcal{J}$ is $(x_1, \dots, x_r)$-*maximal* up to B.

Lemma 4.14. *Let $f \in k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n] \setminus \{0\}$ have $(x_1, \dots, x_r)$-degree at most B. Then there exists a polynomial $g \in k[x_1, \dots, x_r]$ of total degree at most $B \cdot \binom{B+n}{n}$ such that the product $gf \in k[x_1, \dots, x_r, x_{r+1}, \dots, x_n]$ has total degree at most $B\left(1 + \binom{B+n}{n}\right)$.*

Proof. Write f as $\sum_i (\alpha_i/\beta_i) T_i$, where α_i, β_i are coprime in $k[x_1, \dots, x_r]$ and T_i is a power product in $x_{r+1}, \dots, x_n$. Since f has $(x_1, \dots, x_r)$-degree bounded by B, each α_i, β_i, and T_i has total degree at most B. Clear denominators and keep track of the degrees. By Lemma 3.10, there are $\binom{B+n}{n}$ power products of degree at most B in n variables, so f contains at most that many monomials. Let g be $\prod_i \beta_i$, which has total degree at most $B \cdot \binom{B+n}{n}$. It follows that

$$gf = \left(\prod_i \beta_i\right) \cdot \sum_i (\alpha_i/\beta_i) T_i \in k[x_1, \dots, x_r, x_{r+1}, \dots, x_n]$$

and has total degree at most $B\left(1 + \binom{B+n}{n}\right)$. □

Lemma 4.15. *For any d_0, if I is prime up to $\max\left\{b_4(n, d), d_0\left(1 + \binom{d_0+n}{n}\right)\right\}$, then $J = Ik(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$ is $(x_1, \dots, x_r)$-prime up to d_0.*

Proof. Let $g, h \in k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$ each have $(x_1, \dots, x_r)$-degree $\leq d_0$ and suppose $gh \in J$. By Lemma 4.14, there are $g_0, h_0 \in k[x_1, \dots, x_r]$ such that $g_0 g, h_0 h \in k[x_1, \dots, x_n]$ and the total degrees of $g_0 g, h_0 h$ are at most $d_0\left(1 + \binom{d_0+n}{n}\right)$. By Theorem 4.10, $(g_0 g)(h_0 h) \in I$ since $(g_0 g)(h_0 h) \in J \cap k[x_1, \dots, x_n]$ and I is prime up to at least $b_4(n, d)$. Since I is also prime up to at least $d_0\left(1 + \binom{d_0+n}{n}\right)$, either $g_0 g \in I$ or $h_0 h \in I$, showing that either g or h belongs to J. □

Lemma 4.16 (cf. [Schmidt-Göttsch 1989, Lemma 2.3]). *Suppose the $(x_1, \dots, x_r)$-degree of $f \in k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$ is at most d_0, where $d \leq d_0$. For each $j = r+1, \dots, n$, denote by d_j the x_j-degree of the polynomial w_j obtained in Lemma 4.11. There exists $\tilde{f} \in k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$ such that the following hold*:

(1) $\deg_{x_j} \tilde{f} < d_j$,

(2) $f - \tilde{f} \in J = Ik(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$, *and*

(3) *the $(x_1, \dots, x_r)$-degree of $\tilde{f}$ is bounded by $d_0(1 + b_1(n, d))^{n-r}$.*

Proof. The claim follows from successively dividing f by $w_{r+1}, \dots, w_n$. By Lemma 4.11, each such $w_j \in I \cap k[x_1, \dots, x_r][x_j] \subseteq J$ has total degree at most $b_1(n,d)$, so $d_j \le b_1(n,d)$. The first division step involving w_{r+1} at most adds the $(x_1, \dots, x_r)$-degrees of f and w_{r+1} while the x_{r+1}-degree decreases. (If $\deg_{x_{r+1}} f$ is already less than d_{r+1}, we may skip to w_{r+2}.) At each step we increase the original $(x_1, \dots, x_r)$-degree of f (which was at most d_0) by at most $b_1(n,d)$, and we can continue at most d_0-many times. Therefore, the $(x_1, \dots, x_r)$-degree of the remainder after completing division by w_{r+1} is bounded by $d_0 + d_0 \cdot b_1(n,d) = d_0(1+b_1(n,d))$.

After dividing by w_j, the degree of the remainder in x_j is less than d_j and can never increase thereafter because x_j does not appear in w_l for $r < l \ne j$. The remainder $\tilde{f}$ after considering all $n-r$ polynomials w_j thus satisfies the first two claims. The pattern repeats, giving us a bound of

$$d_0 + d_0 \cdot \tbinom{n-r}{1} \cdot b_1(n,d) + \cdots + d_0 \cdot \tbinom{n-r}{n-r-1} \cdot (b_1(n,d))^{n-r-1} + d_0 \cdot (b_1(n,d))^{n-r} = d_0(1+b_1(n,d))^{n-r}$$

when the process terminates. □

Lemma 4.17 (cf. [Schmidt-Göttsch 1989, Lemma 2.4]). *Suppose the $(x_1, \dots, x_r)$-degree of $f \in k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$ is at most d_0, where $d \le d_0$. For each $j = r+1, \dots, n$, denote by d_j the x_j-degree of the polynomial w_j obtained in Lemma 4.11. There is a monic polynomial $\theta_f \in k(x_1, \dots, x_r)[Y]$ such that*

(1) *the Y-degree of θ_f is at most $\prod_{j=r+1}^{n} d_j$,*

(2) *$\theta_f(f) \in J = Ik(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$, and*

(3) *the $(x_1, \dots, x_r)$-degree of θ_f is at most $\left(\prod_{j=r+1}^{n} d_j\right)(d_0(1+b_1(n,d))^{n-r})$.*

Proof. Let $\{v_1, \dots, v_t\}$ be power products in $x_{r+1}, \dots, x_n$ that form a basis of $k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n] \bmod J$. By Lemma 4.11, t is at most $\prod_{j=r+1}^{n} d_j$. By Lemma 4.16, for each v_i and product fv_i there is some $\widetilde{fv_i}$ such that

- for $r < j \le n$, the x_j-degree of $\widetilde{fv_i}$ is less than d_j,
- $fv_i - \widetilde{fv_i} \in J$, and
- $\widetilde{fv_i}$ has $(x_1, \dots, x_r)$-degree at most $d_0(1+b_1(n,d))^{n-r}$.

So we may write

$$\widetilde{fv_i} = \sum_{l=1}^{t} a_{il} v_l,$$

where each $a_{il} \in k(x_1, \dots, x_r)$ has $(x_1, \dots, x_r)$-degree at most $d_0(1+b_1(n,d))^{n-r}$.

We use the determinant trick. Consider the $t \times t$-matrix $A(Y) = [\delta_{il} Y - a_{il}]$ and note that the determinant of $A(Y)$ is monic and $\det(A(f))$ must belong to J: if v is the column vector with entries v_l, then $[a_{il}]v = fv \bmod J$. Therefore $[\delta_{il} f - a_{il}]v = 0 \bmod J$. Multiply both sides by the adjugate of $[\delta_{il} f - a_{il}]$

to obtain $[\delta_{il}\det(A(f))]v \in J$. The power product 1 appears among the v_i, so $\det(A(f)) \in J$.

Let $\theta_f = \det(A(Y))$. Then θ_f has Y-degree at most $\prod_{j=r+1}^{n} d_j$ and $(x_1, \ldots, x_r)$-degree at most $t \cdot (d_0(1+b_1(n,d))^{n-r}) \leq \left(\prod_{j=r+1}^{n} d_j\right)(d_0(1+b_1(n,d))^{n-r})$. □

Theorem 4.18 (cf. [Schmidt-Göttsch 1989, Lemma 2.7]). *Let $d_0 \in \mathbb{N}$ and let*

$$\tilde{d} = \left(\prod_{j=r+1}^{n} d_j\right)(d_0)(1+(1+b_1(n,d))^{n-r}),$$

with d_j defined in Lemma 4.11. If I is prime up to $\max\left\{b_4(n,d), \tilde{d}\left(1+\binom{\tilde{d}+n}{n}\right)\right\}$, then $J = Ik(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ is $(x_1, \ldots, x_r)$-maximal up to d_0.

Proof. Suppose we have $f \in k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n] \setminus J$ with $(x_1, \ldots, x_r)$-degree $\leq d_0$. By Lemma 4.17, there is a monic $\theta_f \in k(x_1, \ldots, x_n)[Y]$ with Y-degree $\leq \prod_{j=r+1}^{n} d_j$ and $(x_1, \ldots, x_r)$-degree $\leq \left(\prod_{j=r+1}^{n} d_j\right)(d_0(1+b_1(n,d))^{n-r})$ so that $\theta_f(f) \in J$. Note that $\theta_f(f)$ has $(x_1, \ldots, x_r)$-degree at most

$$(d_0)\left(\prod_{j=r+1}^{n} d_j\right) + \left(\prod_{j=r+1}^{n} d_j\right)(d_0(1+b_1(n,d))^{n-r}) = \left(\prod_{j=r+1}^{n} d_j\right)(d_0)(1+(1+b_1(n,d))^{n-r}) = \tilde{d}.$$

Let us write $\theta_f = Y^m\theta'$ with m maximal, so $f^m\theta'(f) \in J$. By Lemma 4.15, primality of I up to $\max\left\{b_4(n,d), \tilde{d}\left(1+\binom{\tilde{d}+n}{n}\right)\right\}$ implies $(x_1, \ldots, x_r)$-primality of J up to $\tilde{d}$. Since $f^m\theta'(f)$ has $(x_1, \ldots, x_r)$-degree $\leq \tilde{d}$ and $f \notin J$, we must have $\theta'(f) \in J$. This also implies that the constant term of $\theta'(Y)$ cannot be 0.

Since $\theta'(Y) = Y^s + \sum_{i=1}^{s-1} a_i Y^i + a_0$ with $a_0 \neq 0$ and each $a_i \in k(x_1, \ldots, x_r)$, we have

$$\left(a_0^{-1} f^{s-1} + \sum_{i=1}^{s-1} a_0^{-1} a_i f^{i-1}\right) f + 1 \in J,$$

and therefore f is invertible mod J. □

Corollary 4.19. *Let M be the maximal ideal in Lemma 4.12 and let $d_0, \tilde{d}, I, J$ be defined as in Theorem 4.18, with I being prime up to*

$$\max\left\{b_4(n,d), \tilde{d}\left(1+\binom{\tilde{d}+n}{n}\right)\right\}.$$

If $f \in M \subseteq k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ has total $(x_1, \ldots, x_r)$-degree less than or equal to d_0, then $f \in J$.

Proof. If $f \notin J$, then f is invertible mod J because J is $(x_1, \ldots, x_r)$-maximal up to d_0 by Theorem 4.18. But since $f \in M$, it follows that $1 \in M$, contradicting that M is a proper ideal. □

Proof that $J = M$. We argue that $J = M$ using induction on the number of variables $x_{r+1}, \ldots, x_n$. It is convenient to first treat the case that $x_{r+2} + M, \ldots, x_n + M$ are separable over $k(x_1, \ldots, x_r)$ (technically, the isomorphic copy $k(x_1, \ldots, x_r) + M$ contained in the field $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/M$). Theorem 4.21, which is based on Theorem 2.8 in [Schmidt-Göttsch 1989], contains the heart of the matter.

Lemma 4.20. *Let M be as above and let $M_j := M \cap k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_j]$ for $r+1 \le j \le n$. Then M_j is a maximal ideal of $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_j]$ and the field $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_j]/M_j$ embeds in $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/M$.*

Proof. Consider the generators $x_{r+1} + M, \ldots, x_n + M$ of the field extension $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/M$ over $k(x_1, \ldots, x_r)$. Because each generator is algebraic, the $k(x_1, \ldots, x_r)$-algebra $k(x_1, \ldots, x_r)[x_{r+1} + M, \ldots, x_j + M]$ is a subfield of $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/M$. The $k(x_1, \ldots, x_r)$-algebra is isomorphic to $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_j]/M_j$ via the obvious map sending $x_{r+1} + M_j$ to $x_{r+1} + M$, etc. □

Theorem 4.21 (cf. [Schmidt-Göttsch 1989, Theorem 2.8]). *Take I, J, M as above. Let I be prime up to $b_5(n, d) := (2d)^{2^{3n^2+2n}}$ and $x_{r+2} + M, \ldots, x_n + M$ separable over $k(x_1, \ldots, x_r)$. For each $r+1 \le j \le n$ there are $c_{r+1,j}, \ldots, c_{j,j} \in k[x_1, \ldots, x_r]$, $h_j \in k[x_1, \ldots, x_r][Y]$, and $\phi_{r+1,j}, \ldots, \phi_{j,j} \in k(x_1, \ldots, x_r)[Y]$ such that, if we define $U_j := \sum_{i=r+1}^{j} c_{i,j} x_i$ and $M_j := M \cap k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_j]$, then*

(1) *$U_j + M_j$ generates $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_j]/M_j$ over $k(x_1, \ldots, x_r)$,*

(2) *h_j is the minimal polynomial of $U_j + M_j$ over $k(x_1, \ldots, x_r)$,*

(3) *$h_j(U_j) \in I$ and $x_{r+1} - \phi_{r+1,j}(U_j), \ldots, x_j - \phi_{j,j}(U_j)$ all belong to J, and*

(4) *the total degrees of $c_{r+1,j}, \ldots, c_{j,j} \in k[x_1, \ldots, x_r]$ and $h_j \in k[x_1, \ldots, x_r][Y]$ are at most $b_5(n, d)$.*

Proof. We induct on $r+1 \le j \le n$. Let $w_j(x_j)$ be as defined in Lemma 4.11. For the base case, define $c_{r+1,r+1} = 1$, $h_{r+1} = w_{r+1}(Y)$, and $\phi_{r+1,r+1} = x_{r+1} - w_{r+1}(Y)$. Clearly $U_{r+1} + M_{r+1} = x_{r+1} + M_{r+1}$ generates $k(x_1, \ldots, x_r)[x_{r+1}]/M_{r+1}$ over $k(x_1, \ldots, x_r)$. Lemma 4.11 implies that (2) and (4) hold for $c_{r+1,r+1}$ and h_{r+1}. The bounds suffice since the total degree of w_{r+1} is at most $b_1(n, d) \le 2d^{2^n} \le b_5(n, d)$. Claim (3) holds because $x_{r+1} - \phi_{r+1,r+1}(U_{r+1}) = w_{r+1}(x_{r+1}) \in I \subseteq J$.

Suppose (1)–(4) hold for $U_j, c_{r+1,j}, \ldots, c_{j,j}, h_j$ and $\phi_{r+1,j}, \ldots, \phi_{j,j}$. We may also assume that the total degrees of U_j and h_j are at most $(2d)^{2^{3jn+2j}}$ (this holds for the base case $j = r+1$). Set $c_{r+1,j+1}, \ldots, c_{j,j+1}$ equal to $c_{r+1,j}, \ldots, c_{j,j}$, respectively. By Lemma 4.20, $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_{j+1}]/M_{j+1}$ is a field extending (an isomorphic copy of) $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_j]/M_j$. From the inductive hypothesis, h_j is the minimal polynomial of $U_j + M_{j+1}$ over $k(x_1, \ldots, x_r)$. By assumption $x_{j+1} + M_{j+1}$ is separable and by Lemma 4.11 w_{j+1} is the minimal polynomial of $x_{j+1} + M_{j+1}$ over $k(x_1, \ldots, x_r)$. We also know that $k(x_1, \ldots, x_r)$ is an infinite field

and $U_j + M_j$ generates $k(x_1, \dots, x_r)[x_{r+1}, \dots, x_j]/M_j$. So the primitive element theorem (Theorem 3.2) implies that there exists $c_{j+1,j+1} \in k[x_1, \dots, x_r]$ of total degree at most $(\deg h_j)(b_1(n,d)-1) \leq (2d)^{2^{3jn+2j}} \cdot (2d^{2^n}-1)$ such that $U_{j+1}+M_{j+1} = U_j + c_{j+1,j+1}x_{j+1} + M_{j+1}$ generates $k(x_1, \dots, x_r)[x_{r+1}, \dots, x_{j+1}]/M_{j+1}$ over $k(x_1, \dots, x_r)$. Note that the total degree of U_{j+1} is at most

$$(2d)^{2^{3jn+2j}} \cdot (2d^{2^n} - 1) + 1 \leq (2d)^{2^{3jn+2j}} \cdot 2d^{2^n} \leq (2d)^{2^{3jn+2j}+2^n}.$$

Because $k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]/J$ is a finite-dimensional $k(x_1, \dots, x_r)$-vector space, U_{j+1} is algebraic mod J (and hence mod I). By Theorem 3.25, the set

$$H = \{h \in k[x_1, \dots, x_r][Y] \setminus \{0\} \mid \text{the total degree of } h \text{ is at most } b_1(n+1, \max\{d, \deg U_{j+1}\}) \text{ and } h(U_{j+1}) \in I\}$$

is nonempty. The total degrees of elements of H are bounded by

$$\begin{aligned} &b_1(n+1, \max\{d, \deg U_{j+1}\}) \\ &\quad \leq b_1(n+1, (2d)^{2^{3jn+2j}+2^n}) \leq 2((2d)^{2^{3jn+2j}+2^n})^{2^{n+1}} \\ &\quad \leq (2d)^{(2^{3jn+2j}+2^n)2^{n+1}+1} \leq (2d)^{2^{3jn+2j+n+1}+2^{2n+1}+1} \leq (2d)^{2^{3(j+1)n+2(j+1)}}. \end{aligned}$$

By the same argument we used in Lemma 4.11, there exists some irreducible $h_{j+1} \in H$; by definition of H, the total degree of h_{j+1} is at most

$$(2d)^{2^{3(j+1)n+2(j+1)}} \leq b_5(n,d).$$

(Since $j \leq n$, primality up to $b_5(n,d) := (2d)^{2^{3n^2+2n}}$ suffices for each j. The bound $(2d)^{2^{3(j+1)n+2(j+1)}}$ has the correct form to continue the induction.)

Thus h_{j+1} is the minimal polynomial of $U_{j+1} + M_{j+1}$ over $k(x_1, \dots, x_r)$. Note that $k(x_1, \dots, x_r)[x_{r+1}, \dots, x_{j+1}]/M_{j+1}$ is isomorphic to $k(x_1, \dots, x_r)[Y]/(h_{j+1})$ under the map sending $U_{j+1} + M_{j+1}$ to $Y + (h_{j+1})$.

It remains to define $\phi_{r+1,j+1}, \dots, \phi_{j+1,j+1}$. We start with $\phi_{j+1,j+1}$ and use it to determine the others. Consider the polynomial ring $k(x_1, \dots, x_r)[Y, Z]$. The proof of Theorem 3.2 shows that there exist $A, B \in k(x_1, \dots, x_r)[Y, Z]$ such that

$$\begin{aligned} Z - (x_{j+1} + M_{j+1}) = h_j((U_{j+1} + M_{j+1}) - c_{j+1,j+1}Z)A(U_{j+1} + M_{j+1}, Z) \\ + w_{j+1}(Z)B(U_{j+1} + M_{j+1}, Z). \end{aligned}$$

(This uses the fact that h_j and w_{j+1} are the minimal polynomials of $U_j + M_{j+1} = U_{j+1} - c_{j+1,j+1}x_{j+1} + M_{j+1}$ and $x_{j+1} + M_{j+1}$, respectively.)

Since U_{j+1} generates $k(x_1, \dots, x_r)[x_{r+1}, \dots, x_{j+1}]$ mod M_{j+1}, there is some polynomial $C \in k(x_1, \dots, x_r)[Y]$ such that $x_{j+1} - C(U_{j+1}) \in M_{j+1}$. It follows that

$$\begin{aligned} Z - (C(U_{j+1}) + M_{j+1}) = h_j((U_{j+1} + M_{j+1}) - c_{j+1,j+1}Z)A(U_{j+1} + M_{j+1}, Z) \\ + w_{j+1}(Z)B(U_{j+1} + M_{j+1}, Z). \end{aligned}$$

By the isomorphism sending $U_{j+1} + M_{j+1}$ to $Y + (h_{j+1})$, we have $Z - C(Y) = h_j(Y - c_{j+1,j+1}Z)A(Y, Z) + w_{j+1}(Z)B(Y, Z) + h_{j+1}(Y)D(Y, Z)$ for some D in $k(x_1, \ldots, x_r)[Y, Z]$. Define $\phi_{j+1,j+1}(Y)$ to be $C(Y)$ and observe that upon substituting x_{j+1} for Z and U_{j+1} for Y we get $x_{j+1} - \phi_{j+1,j+1}(U_{j+1}) \in J$.

By the induction hypothesis on (3), $x_{r+1} - \phi_{r+1,j}(U_j), \ldots, x_j - \phi_{j,j}(U_j)$ belong to J. Since $U_j = U_{j+1} - c_{j+1,j+1}x_{j+1}$ and $x_{j+1} - \phi_{j+1,j+1}(U_{j+1}) \in J$, we define $\phi_{l,j+1}(Y)$ to be $\phi_{l,j}(Y - c_{j+1,j+1}\phi_{j+1,j+1}(Y))$ for $r + 1 \le l \le j$. This implies that $x_l - \phi_{l,j+1}(U_{j+1}) \in J$, completing the proof. □

Theorem 4.22. *Let I, J, M be defined as above. Suppose I is prime up to $b_5(n, d)$ and $x_{r+2} + M, \ldots, x_n + M$ are separable over $k(x_1, \ldots, x_r)$. Then J is a maximal ideal of $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$.*

Proof. We prove that $J = M$ by showing for any $p \in k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ that if $p \notin J$, then $p \notin M$ (noting that $J \subseteq M$ by definition). We use the polynomials $U_n, x_{r+1} - \phi_{r+1,n}(U_n), \ldots, x_n - \phi_{n,n}(U_n)$ and $h_n(U_n)$ from Theorem 4.21. By the theorem, $U_n + M_n = U_n + M$ generates the field $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/M$, $x_{r+1} - \phi_{r+1,n}(U_n), \ldots, x_n - \phi_{n,n}(U_n)$ all belong to J, and $h_n(U_n) \in I$ with h_n being the minimal polynomial of $U_n + M$. Hence we may replace, modulo J, each $x_{r+1}, \ldots, x_n$ in p with a polynomial in U_n; i.e., $p = p_1(U_n) + q$ for some $q \in J$ and some $p_1 \in k(x_1, \ldots, x_r)[Y]$. Since $p \notin J$ but $h_n(U_n) \in I$, we know that $p_1(U_n) \notin J$ and the remainder $p_2(U_n)$ from dividing $p_1(U_n)$ by $h_n(U_n)$ is not zero.

Because $p_2(U_n)$ is a nonzero polynomial in U_n of lower degree than $h_n(U_n)$, minimality of h_n implies that $p_2(U_n) \notin M$. Since $p_1(U_n)$ is equal to $p_2(U_n)$ mod J, it follows that $p \notin M$. □

We now reduce the inseparable case to the separable. Theorem 4.25 is based on Theorems 2.8 and 2.12 in [Schmidt-Göttsch 1989]. We use induction, with the base step depending on Theorem 4.22. The inductive step requires a specialization of the faithful flatness results from Section 3A. In Lemma 4.23 we continue to use the same field k and ideals $I \subseteq k[x_1, \ldots, x_r, x_{r+1}, \ldots, x_n]$ and $J \subseteq k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ as before.

Lemma 4.23 (cf. [Schmidt-Göttsch 1989, Lemma 2.10]). *Let $g \in k[x_1, \ldots, x_n]$ have total degree at most $B \ge d$ and let $D = \{t_1, \ldots, t_N\}$ be a set of power products $x_{r+1}^{i_{r+1}} \cdots x_n^{i_n}$, with each element of D having total degree at most B. Suppose there exist $\beta_t \in k(x_1, \ldots, x_r)$ for each $t \in D$ such that $g + \sum_{t \in D} \beta_t t \in J$. Then there exist $\gamma_t \in k(x_1, \ldots, x_r)$ such that $g + \sum_{t \in D} \gamma_t t \in J$ and each γ_t may be written as a ratio of polynomials of total degree at most $\left(2\binom{(2B)^{2^n}+d+n-r}{n-r}B\right)^{2^r}$.*

Proof. Considering g as well as the generators $f_1, \ldots, f_s$ of I as polynomials in $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$, we may apply Theorem 3.5 to conclude that there are $g_i \in k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ having total degree (in $x_{r+1}, \ldots, x_n$) at most

$(2B)^{2^n}$ such that $g + \sum_{t\in D} \beta_t t = \sum_{i=1}^{s} g_i f_i$. The monomials in $x_{r+1}, \dots, x_n$ that appear in the equation have total degree at most $(2B)^{2^n} + d$. By Lemma 3.10, there are

$$N_1 := \binom{(2B)^{2^n}+d+n-r}{n-r}$$

power products in $x_{r+1}, \dots, x_n$ of total degree at most $(2B)^{2^n} + d$.

From the $k(x_1, \dots, x_r)$-coefficients of the power products of $x_{r+1}, \dots, x_n$ in $g + \sum_{t\in D} \beta_t t = \sum_{i=1}^{s} g_i f_i$, we obtain a system of N_1-many linear equations over $k[x_1, \dots, x_r]$ whose coefficients have degree at most B. Theorem 3.6 implies that the system has solutions in $k(x_1, \dots, x_r)$ bounded by $\left(2\binom{(2B)^{2^n}+d+n-r}{n-r}B\right)^{2^r}$. Thus there are $\gamma_t, g_i' \in k(x_1, \dots, x_r)$ that satisfy the claimed bound such that $g + \sum_{t\in D} \gamma_t t = \sum_{i=1}^{s} g_i' f_i \in J$. □

We are ready to handle the general case. To keep track of the bounds, we use the following names in Theorem 4.25. While $b_1(n, d)$, $b_4(n, d)$, and $b_5(n, d)$ are the same as before, note that the other values are not necessarily identical to those in the statements of earlier theorems.

Notation 4.24. Define

$$\begin{aligned}
N_1 &:= \left(2\binom{(2(n-r)b_1(n,d))^{2^n}+d+n-r}{n-r}(n-r)b_1(n,d)\right)^{2^r},\\
N_2 &:= \left(2\binom{(2(n-r)(b_1(n,d))^2)^{2^n}+d+n-r}{n-r}(n-r)(b_1(n,d))^2\right)^{2^r},\\
N_3 &:= b_1(n,d)^{n-r},\\
N_4 &:= N_3N_2 + N_1,\\
N_5 &:= \left(2N_3^2(N_3+1)\binom{N_4+r}{r}(b_1(n,d))^{(r-1)}N_4\right)^{2^r},\\
N_6 &:= N_5 + (n-r)(b_1(n,d))^2,\\
\tilde{d} &:= N_3N_6(1+(1+b_1(n,d))^{n-r}),\\
b_6(n,d) &:= \max\left\{b_4(n,d), b_5(n,d), \tilde{d}\left(1+\binom{\tilde{d}+n}{n}\right)\right\}.
\end{aligned}$$

Theorem 4.25 (cf. [Schmidt-Göttsch 1989, Theorems 2.8 and 2.12]). *If I is prime up to $b_6(n, d)$, then J is a maximal ideal of $k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$.*

Proof. Since I is prime at least up to $b_5(n, d)$, by Theorem 4.22 we are done unless k has prime characteristic p and at least some of $x_{r+1}, \dots, x_n$ are inseparable mod M. For each $r + 1 \le j \le n$, let $h_j(Y) \in k(x_1, \dots, x_r)[Y]$ be the minimal polynomial of x_j mod M. If h_j happens to be separable, define m_j to be 0. If h_j is inseparable, then every exponent of Y that appears in h_j is divisible by p. Let m_j be the greatest power of p such that p^{m_j} divides all exponents of Y that appear in h_j. Recall that the polynomial $w_j(x_j) \in k[x_1, \dots, x_r][x_j]$ from Lemma 4.11 belongs to $I \subseteq M$. Being a minimal polynomial, $h_j(Y)$ divides $w_j(Y)$ in $k(x_1, \dots, x_r)[Y]$. Lemma 4.11 then implies that $p^{m_j} \le \deg_Y(h_j) \le \deg_Y(w_j) = d_j \le b_1(n, d)$.

Let $\tilde{h}_j(Z) \in k(x_1, \ldots, x_r)[Z]$ be the polynomial obtained from h_j by replacing $Y^{p^{m_j}}$ with Z. Note that $\tilde{h}_j$ remains irreducible. It follows from our choice of m_j that not every exponent of Z appearing in $\tilde{h}_j$ is divisible by p. Hence $\tilde{h}_j$ is the minimal polynomial of $x_j^{p^{m_j}} \bmod M$ and $x_j^{p^{m_j}} + M$ is separable over $k(x_1, \ldots, x_r)$.

Let $m = \max\{m_{r+1}, \ldots, m_n\}$. For convenience, let us define the polynomial ring

$$P_{r,l,n} := k(x_1, \ldots, x_r)\left[x_{r+1}, \ldots, x_l, x_{l+1}^{p^m}, \ldots, x_n^{p^m}\right]$$

(where $P_{r,r,n}$ is understood to be $k(x_1, \ldots, x_r)\left[x_{r+1}^{p^m}, \ldots, x_n^{p^m}\right]$. Note that $M \cap P_{r,r,n}$ is still a maximal ideal: if $f \in P_{r,r,n} \setminus M$, then by maximality of M, there exists $g \in k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ such that $fg - 1 \in M$. Since k has prime characteristic p, $(fg-1)^{p^m} = f^{p^m} g^{p^m} - 1 = f(f^{p^m-1} g^{p^m}) - 1 \in M$, with $f^{p^m-1} g^{p^m} \in P_{r,r,n}$. This shows that $M \cap P_{r,r,n}$ is maximal. Since $x_{r+1}^{p^m} + M \cap P_{r,r,n}, \ldots, x_n^{p^m} + M \cap P_{r,r,n}$ are separable over $k(x_1, \ldots, x_r)$, by Theorem 4.22 the ideal $J \cap P_{r,r,n} = M \cap P_{r,r,n}$. We use induction to show that $J = M$.

For $r \le l \le n$, define $S_l = J \cap P_{r,l,n}$ and $M_l = M \cap P_{r,l,n}$. (So in particular $M_n = M \cap k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n] = M$.) As was the case with $l = r$, each M_l is a maximal ideal of $P_{r,l,n}$. Define the quotient rings

$$A_l = P_{r,l,n}/S_l \quad \text{and} \quad B_l = P_{r,l,n}/M_l.$$

The previous paragraph established that $S_r = M_r$, the base case of our induction. Now suppose that $S_j = M_j$ for some $r \le j < n$. In particular, $A_j = B_j$. We claim that $S_{j+1} = M_{j+1}$.

Note that A_{j+1} surjects as a ring onto the field B_{j+1} via the natural map sending $\alpha + S_{j+1}$ to $\alpha + M_{j+1}$ for $\alpha \in P_{r,j+1,n}$. We prove this map is injective by showing that the vector space dimension of B_{j+1} over B_j is greater than or equal to that of A_{j+1} over the field $A_j = B_j$. This will show that $A_{j+1} = B_{j+1}$ and $S_{j+1} = M_{j+1}$.

Since $x_{j+1}^{p^m} + M_{j+1} \in B_j$ and B_{j+1} is generated as a field over B_j by $x_{j+1} + M_{j+1}$, B_{j+1}/B_j is a purely inseparable extension. Hence the minimal polynomial of $x_{j+1} + M_{j+1}$ over B_j has the form $X^{p^\mu} + b$ for some $\mu \in \mathbb{N}$ and $b \in B_j$. In particular, the degree of the extension B_{j+1}/B_j is p^μ. It remains to show that the vector space dimension of A_{j+1} over $A_j = B_j$ is at most p^μ.

Denote by τ the minimal natural number such that $x_{j+1}^{p^\tau} + S_{j+1} \in A_j$. Note that $\mu \le \tau \le m$. Let $D = \{t_1 + S_j, \ldots, t_N + S_j\}$ be a $k(x_1, \ldots, x_r)$-basis of $A_j = B_j$, where $t_1, \ldots, t_N$ are representative power products in the variables $x_{r+1}, \ldots x_j, x_{j+1}^{p^m}, \ldots, x_n^{p^m}$. Thus there are $\alpha_t, \beta_t \in k(x_1, \ldots, x_r)$ such that

$$x_{j+1}^{p^\mu} + \textstyle\sum_{t \in D} \alpha_t t \in M \quad \text{and} \quad x_{j+1}^{p^\tau} + \sum_{t \in D} \beta_t t \in J.$$

(From now on we write $t \in D$ to refer to any of $t_1, \ldots, t_N$.) It follows from Lemma 4.11 that we may assume that a power product $t \in D$ has total degree at most $(n-r)b_1(n,d)$ as a polynomial in $x_{r+1}, \ldots x_j, x_{j+1}^{p^m}, \ldots, x_n^{p^m}$. We have

$p^\tau \leq p^m \leq b_1(n,d)$, so by Lemma 4.23 we may assume that the β_t are ratios of polynomials of total degree at most

$$N_1 := \left(2\binom{(2(n-r)b_1(n,d))^{2^n}+d+n-r}{n-r}(n-r)b_1(n,d)\right)^{2^r}.$$

If $\tau = \mu$, then $x_{j+1}^{p^\tau} + \sum_{t\in D}\beta_t t \in J$ implies that the dimension of A_{j+1} over A_j is at most p^μ. Hence it suffices to obtain a contradiction from the assumption $\mu < \tau$. Suppose then that $\mu < \tau$ and consider

$$(1)\qquad \left(x_{j+1}^{p^\mu} + \sum_{t\in D}\alpha_t t\right)^{p^{\tau-\mu}} - \left(x_{j+1}^{p^\tau} + \sum_{t\in D}\beta_t t\right) = \sum_{t\in D}\alpha_t^{p^{\tau-\mu}} t^{p^{\tau-\mu}} - \sum_{t\in D}\beta_t t.$$

This belongs to $M_j = M \cap P_{r,j,n}$, which by hypothesis equals $S_j = J \cap P_{r,j,n}$. By Lemma 4.23 we see that for each $t \in D$, there exist $\gamma_{t,t'} \in k(x_1,\dots,x_r)$ such that $t^{p^{\tau-\mu}} = \sum_{t'\in D}\gamma_{t,t'}t' \bmod S_j$ and $\gamma_{t,t'}$ is a ratio of polynomials having total degree at most

$$N_2 := \left(2\binom{(2(n-r)(b_1(n,d))^2)^{2^n}+d+n-r}{n-r}(n-r)(b_1(n,d))^2\right)^{2^r}.$$

Substituting $\sum_{t'\in D}\gamma_{t,t'}t'$ for $t^{p^{\tau-\mu}}$, we get the following equalities mod S_j:

$$(2)\qquad \sum_{t'\in D}\beta_{t'}t' = \sum_{t\in D}\beta_t t = \sum_{t\in D}\alpha_t^{p^{\tau-\mu}} t^{p^{\tau-\mu}} = \sum_{t\in D}\alpha_t^{p^{\tau-\mu}}\left(\sum_{t'\in D}\gamma_{t,t'}t'\right)$$
$$= \sum_{t\in D}\sum_{t'\in D}\left(\alpha_t^{p^{\tau-\mu}}\gamma_{t,t'}t'\right) = \sum_{t'\in D}\left(\sum_{t\in D}\alpha_t^{p^{\tau-\mu}}\gamma_{t,t'}\right)t'.$$

The $t_i + S_j$ form a $k(x_1,\dots,x_r)$-basis of $A_j = B_j$, so for each $t' \in D$, we have

$$\sum_{t\in D}\alpha_t^{p^{\tau-\mu}}\gamma_{t,t'} = \beta_{t'}.$$

Note that the cardinality $|D|$ of D is at most $N_3 := b_1(n,d)^{n-r}$ because each variable $x_{r+1},\dots,x_j,x_{j+1}^{p^m},\dots,x_n^{p^m}$ in t has power at most $b_1(n,d)$. Clearing denominators in each equation (separately for each t'), we obtain a system of equations

$$\left\{\sum_{t\in D}\alpha_t^{p^{\tau-\mu}}\widetilde{\gamma}_{t,t'} = \widetilde{\beta}_{t'}\right\}_{t'\in D}$$

such that $\widetilde{\gamma}_{t,t'}, \widetilde{\beta}_{t'} \in k[x_1,\dots,x_r]$ and have total degree at most $N_4 := N_3N_2 + N_1$.

By Theorem 3.8, for each $t \in D$ there exists $\widetilde{\alpha}_t \in k(x_1,\dots,x_r)$ that is a ratio of polynomials of total degree at most $N_5 := \left(2N_3^2(N_3+1)\binom{N_4+r}{r}p^{(\tau-\mu)(r-1)}N_4\right)^{2^r}$ satisfying $\left\{\sum_{t\in D}\widetilde{\alpha}_t^{p^{\tau-\mu}}\widetilde{\gamma}_{t,t'} = \widetilde{\beta}_{t'}\right\}_{t'\in D}$. Dividing to "unclear denominators", we have

$$\left\{\sum_{t\in D}\widetilde{\alpha}_t^{p^{\tau-\mu}}\gamma_{t,t'} = \beta_{t'}\right\}_{t'\in D}.$$

Referring to the equalities in (1) and (2) and substituting for $\beta_{t'}$, we obtain the following equalities mod S_j:

$$\begin{aligned}\sum_{t\in D}\alpha_t^{p^{\tau-\mu}}t^{p^{\tau-\mu}} &= \sum_{t\in D}\beta_t t \;=\; \sum_{t'\in D}\beta_{t'}t' \\ &= \sum_{t'\in D}\Big(\sum_{t\in D}\widetilde{\alpha}_t^{p^{\tau-\mu}}\gamma_{t,t'}\Big)t' = \sum_{t'\in D}\sum_{t\in D}\big(\widetilde{\alpha}_t^{p^{\tau-\mu}}\gamma_{t,t'}t'\big) \\ &= \sum_{t\in D}\widetilde{\alpha}_t^{p^{\tau-\mu}}\Big(\sum_{t'\in D}\gamma_{t,t'}t'\Big) = \sum_{t\in D}\widetilde{\alpha}_t^{p^{\tau-\mu}}t^{p^{\tau-\mu}} = \sum_{t\in D}(\widetilde{\alpha}_t t)^{p^{\tau-\mu}}.\end{aligned}$$

Since $\tau-\mu>0$ by assumption, $p^{\tau-\mu}$-th roots are unique and $\sum_{t\in D}\alpha_t t = \sum_{t\in D}\widetilde{\alpha}_t t \bmod S_j$. It follows that $x_{j+1}^{p^\mu}+\sum_{t\in D}\widetilde{\alpha}_t t\in M$. Observe that the $(x_1,\dots,x_r)$-degree of this polynomial is at most $N_6 := N_5+(n-r)(b_1(n,d))^2$. Let d_0 in Corollary 4.19 be N_6 and consequently define

$$\tilde{d} := (b_1(n,d)^{n-r})(d_0)(1+(1+b_1(n,d))^{n-r}) = N_3N_6(1+(1+b_1(n,d))^{n-r}).$$

Since I is prime up to $b_6(n,d) := \max\{b_4(n,d), b_5(n,d), \tilde{d}(1+\binom{\tilde{d}+n}{n})\}$, we have by Corollary 4.19 that $x_{j+1}^{p^\mu}+\sum_{t\in D}\widetilde{\alpha}_t t$ is in J, in fact in $S_{j+1}=J\cap P_{r,j+1,n}$. Thus $x_{j+1}^{p^\mu}+S_{j+1}\in A_j$, contradicting the minimality of τ and proving that $S_{j+1}=M_{j+1}$. By induction, $J=S_n=M_n=M$ and J is maximal. □

4C. ***Polynomial bounds on primality.*** Let $b(n,d)$ be the function $b_6(n,d)$ from the preceding theorem.

Theorem 4.26. *If I is prime up to $b(n,d)$, then I is prime.*

Proof. The cases $n=1$ and $d=1$ are covered by Theorem 4.2. If $n,d>1$, then $J\cap k[x_1,\dots,x_n]=I$ by Theorem 4.10. The ideal J is maximal by Theorem 4.25 and restrictions of prime ideals to subrings are prime, so I is prime. □

We conclude this section with concrete upper bounds on $b(n,d)$. For each lemma the claimed bound is greater than d, so the cases $n=1$ and $d=1$ are covered and we may assume $n,d>1$ where necessary.

Lemma 4.27. $b_4(n,d)\le(2nd)^{n2^{4n+8}}$ *for all* $n,d\ge 1$.

Proof. Using earlier bounds on $b_1(n,d)$ and $b_3(n,d)$ we obtain

$$\begin{aligned}b_4(n,d) &= b_1(n+1,(n-1)\cdot b_3(n,d)+1) \le 2((n-1)\cdot b_3(n,d)+1)^{2^{n+1}} \\ &\le 2\big((n-1)\cdot 2^{n2^{2n+6}}d^{n2^{3n+2}}+1\big)^{2^{n+1}} \le 2\big(n2^{n2^{2n+6}}d^{n2^{3n+2}}\big)^{2^{n+1}} \\ &\le \big(n2^{n2^{2n+7}}d^{n2^{3n+2}}\big)^{2^{n+1}} \le (2nd)^{n2^{4n+8}}.\end{aligned}$$

□

Similarly, we obtain bounds on the values defined in Notation 4.24:

Lemma 4.28. $N_1\le N_2\le(2nd)^{n2^{3n+2}}$.

Proof. Clearly $N_1 \leq N_2$. For the second inequality, compute

$$\begin{aligned}
N_2 &= \left(2\binom{(2(n-r)(b_1(n,d))^2)^{2^n}+d+n-r}{n-r}(n-r)(b_1(n,d))^2\right)^{2^r} \\
&\leq \left(2\binom{(2n(b_1(n,d))^2)^{2^n}+d+n}{n}(n)(b_1(n,d))^2\right)^{2^n} \\
&\leq \left(2\binom{(2n(2d^{2^n})^2)^{2^n}+d+n}{n}(n)(2d^{2^n})^2\right)^{2^n} \\
&\leq \left(2\left((2n(2d^{2^n})^2)^{2^n}+d+n\right)^n(n)(2d^{2^n})^2\right)^{2^n} \\
&\leq \left(2\left(2(2n(2d^{2^n})^2)^{2^n}\right)^n(n)(2d^{2^n})^2\right)^{2^n} \\
&\leq 2^{5n2^{2n+1}}n^{2n2^{2n}}d^{2n2^{3n+1}} \leq (2nd)^{n2^{3n+2}}.
\end{aligned}$$

□

Lemma 4.29. $N_3 \leq 2^n d^{n2^n}$.

Proof. We have

$$N_3 = b_1(n,d)^{n-r} \leq b_1(n,d)^n \leq (2d^{2^n})^n = 2^n d^{n2^n}.$$

□

Lemma 4.30. $N_4 \leq (2nd)^{n2^{3n+3}}$.

Proof. We compute

$$\begin{aligned}
N_4 &= N_3N_2 + N_1 \leq N_2(N_3+1) \leq (2nd)^{n2^{3n+2}}(2^n d^{n2^n}+1) \\
&\leq (2nd)^{n2^{3n+2}}(2^{n+1}d^{n2^n}) \leq (2nd)^{n2^{3n+3}}.
\end{aligned}$$

□

Lemma 4.31. $N_5 \leq (2nd)^{n(n+1)2^{4n+4}}$.

Proof. We compute

$$\begin{aligned}
N_5 &= (2N_3^2(N_3+1)\tbinom{N_4+r}{r}(b_1(n,d))^{(r-1)}N_4)^{2^r} \\
&\leq \left(2^2N_3^3\tbinom{N_4+n}{n}(2d^{2^n})^{(n-1)}N_4\right)^{2^n} \\
&\leq \left(2^2N_3^3(N_4+n)^n(2d^{2^n})^{(n-1)}N_4\right)^{2^n} \\
&\leq \left(2^2N_3^3(2N_4)^n(2d^{2^n})^{(n-1)}N_4\right)^{2^n} \\
&\leq \left(2^2(2^n d^{n2^n})^3(2((2nd)^{n2^{3n+3}}))^n(2d^{2^n})^{(n-1)}(2nd)^{n2^{3n+3}}\right)^{2^n} \\
&\leq 2^{(1+2n)2^n}(2^n d^{n2^n})^{3\cdot 2^n}((2nd)^{n2^{3n+3}})^{(n+1)2^n}d^{(n-1)2^{2n}} \\
&\leq 2^{(1+2n)2^n+3n2^n+n(n+1)2^{4n+3}}n^{n(n+1)2^{4n+3}}d^{3n2^{2n}+n(n+1)2^{4n+3}+(n-1)2^{2n}} \\
&\leq (2nd)^{(4n-1)2^{2n}+n(n+1)2^{4n+3}} \leq (2nd)^{n(n+1)2^{4n+4}}.
\end{aligned}$$

□

Lemma 4.32. $N_6 \leq 2(2nd)^{n(n+1)2^{4n+4}}$.

Proof. We have

$$\begin{aligned} N_6 &= N_5 + (n-r)(b_1(n,d))^2 \le N_5 + n(2d^{2^n})^2 \\ &\le (2nd)^{n(n+1)2^{4n+4}} + n2^2 d^{2^{n+1}} \le 2(2nd)^{n(n+1)2^{4n+4}}. \end{aligned}$$ □

Lemma 4.33. $\tilde{d} \le (2nd)^{n(n+1)2^{4n+5}}$.

Proof. We compute

$$\begin{aligned} \tilde{d} &= N_3 N_6 (1 + (1 + b_1(n,d))^{n-r}) \le N_3 N_6 (1 + (1 + 2d^{2^n})^n) \le N_3 N_6 (2^{2n+1} d^{n2^n}) \\ &\le (2^n d^{n2^n})(2(2nd)^{n(n+1)2^{4n+4}})(2^{2n+1} d^{n2^n}) \\ &\le 2^{3n+2+n(n+1)2^{4n+4}} n^{n(n+1)2^{4n+4}} d^{2n2^n + n(n+1)2^{4n+4}} \\ &\le (2nd)^{n(n+1)2^{4n+5}}. \end{aligned}$$ □

Lemma 4.34. $\tilde{d}\big(1 + \binom{\tilde{d}+n}{n}\big) \le (2nd)^{n(n+1)^2 2^{4n+6}}$.

Proof. We have

$$\begin{aligned} \tilde{d}\big(1 + \tbinom{\tilde{d}+n}{n}\big) &\le \tilde{d}(1 + (\tilde{d}+n)^n) \le \tilde{d}(1 + (2\tilde{d})^n) \le (2\tilde{d})^{n+1} \\ &\le \big(2(2nd)^{n(n+1)2^{4n+5}}\big)^{n+1} \le (2nd)^{n(n+1)^2 2^{4n+6}}. \end{aligned}$$ □

Theorem 4.35. $b(n,d) \le \max\big\{(2d)^{2^{3n^2+2n}}, (2nd)^{n(n+1)^2 2^{4n+6}}\big\}$ *for all* $n, d \ge 1$.

Proof. We have

$$\begin{aligned} b(n,d) = b_6(n,d) &= \max\big\{b_4(n,d), b_5(n,d), \tilde{d}\big(1 + \tbinom{\tilde{d}+n}{n}\big)\big\} \\ &\le \max\big\{(2nd)^{n2^{4n+8}}, (2d)^{2^{3n^2+2n}}, (2nd)^{n(n+1)^2 2^{4n+6}}\big\} \\ &\le \max\big\{(2d)^{2^{3n^2+2n}}, (2nd)^{n(n+1)^2 2^{4n+6}}\big\}. \end{aligned}$$ □

If desired, one can continue to simplify and obtain larger, more-readable bounds:

Corollary 4.36. $b(n,d) \le (2nd)^{n^3 2^{6n^2}}$ *for all* $n, d \ge 1$.

Proof. We have

$$\begin{aligned} b(n,d) &\le \max\big\{(2d)^{2^{3n^2+2n}}, (2nd)^{n(n+1)^2 2^{4n+6}}\big\} \\ &\le (2nd)^{\max\{2^{3n^2+2n},\, n(n+1)^2 2^{4n+6}\}} \le (2nd)^{n(n+1)^2 2^{3n^2+2n}} \\ &\le (2nd)^{n^3 2^{3n^2+2n+2}} \le (2nd)^{n^3 2^{6n^2}}. \end{aligned}$$ □

5. Maximal Ideals

We note that an analogous result, with a simpler proof, holds for maximal ideals: if an ideal is *maximal up to b* (see Definition 4.1) for large enough b, then the ideal is maximal. Similar remarks apply to the following proof and an ultraproduct argument of Schoutens [2010, 4.1.4] as held for Theorem 1.1 and Schmidt-Göttsch's argument mentioned in the introduction.

The following lemma is a standard step in the proof of the Noether normalization theorem (see, e.g., [Crespo and Hajto 2011, Proposition 1.1.8]):

Lemma 5.1. *Let $f \in k[x_1, \dots, x_n]$ be a nonzero polynomial of total degree d over a field k. There is some $c \in k \setminus \{0\}$ and $a_1, \dots, a_{n-1} \leq (d+1)^{n-1}$ such that the polynomial*

$$cf(y_1 + y_n^{a_1}, y_2 + y_n^{a_2}, \dots, y_{n-1} + y_n^{a_{n-1}}, y_n)$$

is monic in y_n.

To streamline the main proof we first take care of the simple cases and prove a technical inequality.

Lemma 5.2. *For any field k and any proper ideal $I \subseteq k[x_1, \dots, x_n]$ with generators of degree 1, if I is maximal up to 1, then I is maximal. If $n = 1$ and I is proper with generators of degree at most $d \geq 1$, then maximality up to d suffices.*

Proof. Suppose the generators of I have degree 1. By an invertible affine change of variables, we may assume that the generators have the form $x_1, \dots, x_m$ for some $m \leq n$. (Such a change of variables preserves our assumption that linear polynomials not in the ideal are invertible modulo the ideal.) If $m < n$, then x_{m+1} is invertible mod I and $x_{m+1} f - 1 \in I$ for some f. However, $I = (x_1, \dots, x_m)$ cannot have an element with nonzero constant term. Hence $m = n$ and I is maximal.

In the case $n = 1$, $k[x_1]$ is a PID and $I = (f)$ for some f of degree at most d. If $f = 0$, then x is not invertible mod I and I is not maximal up to d. Otherwise, reduction by f gives a nonzero remainder of degree less than d for every element of $k[x_1] \setminus I$. Hence maximality up to d implies that I is maximal. □

Lemma 5.3. *Let k, n, d be natural numbers such that $3 < k + 1 < n$ and $d \geq 1$. Define $D := (2d)^{n(n-1)\cdots(n-k)2^{(k-1)n}}$. Then*

$$(2D)^{(n-k-1)2^{(n-k+2)}} \leq (2d)^{n(n-1)\cdots(n-k)(n-k-1)2^{kn}}.$$

Proof. Applying the definition of D and simplifying, we convert the left side of the claimed inequality into

$$2^{(n-k-1)2^{n-k+2}} (2d)^{n\cdots(n-k-1)2^{kn-k+2}}.$$

Dividing by $(2d)^{n\cdots(n-k-1)2^{kn-k+2}}$ and simplifying, we see the claimed inequality is equivalent to

$$\begin{aligned} 2^{(n-k-1)2^{n-k+2}} &\leq ((2d)^{n(n-1)\cdots(n-k)(n-k-1)})^{(2^{kn}-2^{kn-k+2})} \\ &= ((2d)^{n(n-1)\cdots(n-k)(n-k-1)})^{(2^{kn-k+2})(2^{k-2}-1)}, \end{aligned}$$

which is clear since $k > 2$. □

Theorem 5.4. *Define* $m(n,d) := (2d)^{(n-1)(n!)2^{(n-2)n}}$ *for all* $n > 2$, $d > 1$. *Otherwise let* $m(n,1) := 1$ *(for any* n*) and* $m(1,d) := d$, $m(2,d) := 4d^4$ *if* $d > 1$. *For any field* k *and any proper ideal* $I \subseteq k[x_1,\ldots,x_n]$ *with generators of total degree at most* d, *if* I *is maximal up to* $m(n,d)$, *then* I *is maximal.*

Proof. By Lemma 5.2, bounds of $m(n,1) = 1$ and $m(1,d) = d$ suffice if $d = 1$ or $n = 1$ and $d > 1$, respectively. Thus we may assume $n, d > 1$; by Theorem 3.18 $b_1(n,d) \leq 2d^{2^n}$.

The Noether normalization theorem applied to $R = k[x_1,\ldots,x_n]/I$ states that there is an injective homomorphism $\pi : k[z_1,\ldots,z_r] \to R$ such that R is a finite extension of a polynomial ring $k[z_1,\ldots,z_r]$ for some $0 \leq r \leq n$. The usual proof proceeds by induction on the number of generators n of R as a k-algebra. We reproduce the argument but keep track of bounds along the way. Our first goal is to show that in our scenario, bounded maximality forces r to be 0.

Toward a contradiction, suppose $r > 0$. By maximality up to $m(n,d)$, the ideal I must be nonzero. Starting with a nonzero generator of degree at most d, Lemma 5.1 changes variables by substituting $y_i + y_n^{a_i}$ for x_i if $i < n$ and y_n for x_n using some integers $a_i \leq (d+1)^{n-1}$ such that the transformed generator is monic in y_n. This yields generators of degree at most $(d+1)^{n-1} \cdot d \leq (d+1)^n$ for the ideal $\tilde{I}$ in $k[y_1,\ldots,y_n]$ generated by the generators of I (after substitution). The induction continues if there is a nontrivial relation between $y_1,\ldots,y_{n-1}$; i.e., if the elimination ideal obtained by eliminating y_n from $\tilde{I}$ is nonzero. Otherwise $\pi(z_i) = (x_i - x_n^{a_i}) + I$ for $i < n$ gives the claimed map; note that $x_n + I$ is integral over $\pi(k[z_1,\ldots,x_{n-1}])$. By hypothesis, the process stops after at most $n-1$ steps, leaving us with the desired map for some $r \geq 1$ and $k[z_1,\ldots,z_r]$. Theorem 3.24 implies that the generators of the elimination ideal are bounded by $b_1(n,(d+1)^n)$ after one step of substitution and elimination, $b_1\big(n-1,(b_1(n,(d+1)^n)+1)^{n-1}\big)$ after two, and so on.

We analyze the alternating substitution and elimination steps to bound the degrees of (representatives of) $\pi(z_1),\ldots,\pi(z_r)$ as polynomials in the variables $x_1,\ldots,x_n$. Let $E_n = d$. Define D_{n-k} to be $(E_{n-k+1}+1)^{n-k}$ and E_{n-k} to be $2(D_{n-k}\cdot E_{n-k+1})^{2^{n-k+1}}$ for $0 < k < n$. By induction, D_{n-k} is a bound on the degree of a substitution at the k-th step and E_{n-k} is a bound on the degree of the generators after k-many steps of substitution and elimination. Since we seek the degrees of

the images of $z_1, \dots, z_r$ in the original variables (and not just the variables in the preceding step), our goal is to bound the product $\prod_{i=1}^{n-1} D_{n-i}$. (We eliminate at most $n-1$ variables lest $r = 0$.)

Note that $E_{n-k+1} \leq D_{n-k}$ and so

$$E_{n-k} \leq 2(D_{n-k}^2)^{2^{n-k+1}} = 2(D_{n-k})^{2^{n-k+2}}$$

for all $0 < k < n$. It follows that $E_{n-k+1} \leq 2(D_{n-k+1})^{2^{n-k+3}}$ and hence

$$D_{n-k} \leq \left(2(D_{n-k+1})^{2^{n-k+3}} + 1\right)^{n-k} \leq \left(2^2(D_{n-k+1})^{2^{n-k+3}}\right)^{n-k} \leq (2D_{n-k+1})^{(n-k)2^{n-k+3}}$$

for $1 < k < n$.

It is immediate from the definitions that $D_{n-1} = (d+1)^{n-1} \leq (2d)^{n(n-1)}$, and a calculation like that of Lemma 5.3 shows that $D_{n-2} \leq (2d)^{n(n-1)(n-2)2^n}$. Using Lemma 5.3 and the inequality $D_{n-k} \leq (2D_{n-k+1})^{(n-k)2^{n-k+3}}$ for induction on k, we find that

$$D_{n-k} \leq (2d)^{n(n-1)\cdots(n-k)2^{(k-1)n}}$$

for $2 < k < n$; the previous sentence establishes the inequality for $k = 1, 2$. It follows that $\prod_{i=1}^{k} D_{n-i} \leq (2d)^{kn(n-1)\cdots(n-k)2^{(k-1)n}}$ and so $\pi(z_1), \dots, \pi(z_r)$ can be represented by polynomials of degree at most $(2d)^{(n-1)(n!)2^{(n-2)n}}$ in $x_1, \dots, x_n$. One may easily check that $(2d)^{(n-1)(n!)2^{(n-2)n}} \leq m(n,d)$ for all $n, d > 1$.

Then since I is maximal up to $m(n,d)$, $\pi(z_r)$ is invertible in R ($z_r \neq 0$, so by injectivity of π we know $\pi(z_r) \notin I$). Since R is integral over $\pi(k[z_1, \dots, z_r])$, $(\pi(z_r))^{-1}$ is a root of a monic equation with coefficients in $\pi(k[z_1, \dots, z_r])$. Multiplying the monic equation by an appropriate power of $\pi(z_r)$ shows that $(\pi(z_r))^{-1} \in \pi(k[z_1, \dots, z_r])$, whence z_r is invertible in $k[z_1, \dots, z_r]$. But this is absurd, so r is equal to 0 and R is finite over k.

Since R is finite over k, for each $x_1, \dots, x_n$ the restricted ideal $I \cap k[x_i]$ is nonzero. By Theorem 3.24 there is a nonzero polynomial $\alpha_i(x_i) \in I \cap k[x_i]$ of degree at most $b_1(n,d)$ for each $x_1, \dots, x_n$. Using α_i to reduce higher powers of x_i mod I, we see that any $f \notin I$ is equivalent mod I to some $\tilde{f} \notin I$ of total degree at most $nb_1(n,d) \leq m(n,d)$ for $n, d > 1$. By maximality up to $m(n,d)$, f is invertible mod I and hence I is maximal. □

A single formula for the bound easily follows:

Corollary 5.5. *$m(n,d) \leq (2d)^{n(n!)2^{(n-1)n}}$ for all $n, d \geq 1$.*

References

[Adams and Loustaunau 1994] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Grad. Studies in Math. **3**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Aschenbrenner 2004] M. Aschenbrenner, "Ideal membership in polynomial rings over the integers", *J. Amer. Math. Soc.* **17**:2 (2004), 407–441. MR Zbl

[Becker and Weispfenning 1993] T. Becker and V. Weispfenning, *Gröbner bases: a computational approach to commutative algebra*, Grad. Texts in Math. **141**, Springer, 1993. MR Zbl

[Buchberger 1965] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, Universität Innsbruck, 1965, available at https://tinyurl.com/buchberphd.

[Buchberger and Winkler 1998] B. Buchberger and F. Winkler (editors), *Gröbner bases and applications* (Linz, Austria, 1998), Lond. Math. Soc. Lect. Note Ser. **251**, Cambridge Univ. Press, 1998. MR Zbl

[Chistov 2008] A. L. Chistov, "Double-exponential lower bound for the degree of any system of generators of a polynomial prime ideal", *Algebra i Analiz* **20**:6 (2008), 186–213. In Russian; translated in *St. Petersburg Math. J.* **20**:6 (2009), 983–1001. MR Zbl

[Cox et al. 1992] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, Springer, 1992. MR Zbl

[Crespo and Hajto 2011] T. Crespo and Z. Hajto, *Algebraic groups and differential Galois theory*, Grad. Studies in Math. **122**, Amer. Math. Soc., Providence, RI, 2011. MR Zbl

[van den Dries and Schmidt 1984] L. van den Dries and K. Schmidt, "Bounds in the theory of polynomial rings over fields: a nonstandard approach", *Invent. Math.* **76**:1 (1984), 77–91. MR Zbl

[Dubé 1990] T. W. Dubé, "The structure of polynomial ideals and Gröbner bases", *SIAM J. Comput.* **19**:4 (1990), 750–775. MR Zbl

[Eisenbud et al. 1992] D. Eisenbud, C. Huneke, and W. Vasconcelos, "Direct methods for primary decomposition", *Invent. Math.* **110**:2 (1992), 207–235. MR Zbl

[Figueira et al. 2011] D. Figueira, S. Figueira, S. Schmitz, and P. Schnoebelen, "Ackermannian and primitive-recursive bounds with Dickson's lemma", pp. 269–278 in *26th Annual IEEE Symposium on Logic in Computer Science* (Toronto, 2011), IEEE, Los Alamitos, CA, 2011. MR

[Fröhlich and Shepherdson 1955] A. Fröhlich and J. C. Shepherdson, "On the factorisation of polynomials in a finite number of steps", *Math. Z.* **62** (1955), 331–334. MR Zbl

[Gianni et al. 1988] P. Gianni, B. Trager, and G. Zacharias, "Gröbner bases and primary decomposition of polynomial ideals", *J. Symbolic Comput.* **6**:2-3 (1988), 149–167. MR Zbl

[Göral 2018] H. Göral, "Height bounds, Nullstellensatz and primality", *Comm. Algebra* **46**:10 (2018), 4463–4472. MR Zbl

[Harrison-Trainor et al. 2012] M. Harrison-Trainor, J. Klys, and R. Moosa, "Nonstandard methods for bounds in differential polynomial rings", *J. Algebra* **360** (2012), 71–86. MR Zbl

[Hermann 1926] G. Hermann, "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale", *Math. Ann.* **95**:1 (1926), 736–788. MR Zbl

[Hermann 1998] G. Hermann, "The question of finitely many steps in polynomial ideal theory", *ACM SIGSAM Bull.* **32**:3 (1998), 8–30. Zbl

[Kohlenbach 2008] U. Kohlenbach, *Applied proof theory: proof interpretations and their use in mathematics*, Springer, 2008. MR Zbl

[Kreuzer and Robbiano 2000] M. Kreuzer and L. Robbiano, *Computational commutative algebra, I*, Springer, 2000. MR Zbl

[Lang 1965] S. Lang, *Algebra*, Addison-Wesley, Reading, MA, 1965. MR Zbl

[León Sánchez and Ovchinnikov 2016] O. León Sánchez and A. Ovchinnikov, "On bounds for the effective differential Nullstellensatz", *J. Algebra* **449** (2016), 1–21. MR Zbl

[Mayr and Meyer 1982] E. W. Mayr and A. R. Meyer, "The complexity of the word problems for commutative semigroups and polynomial ideals", *Adv. Math.* **46**:3 (1982), 305–329. MR Zbl

[Renschuch 1980] B. Renschuch, "Beiträge zur konstruktiven Theorie der Polynomideale, XVII-1: Zur Hentzelt–Noether–Hermannschen Theorie der endlich vielen Schritte", *Wiss. Z. Pädagog. Hochsch. "Karl Liebknecht" Potsdam* **24**:1 (1980), 87–99. MR Zbl

[Robbiano 1991] L. Robbiano, "Bounds for degrees and number of elements in Gröbner bases", pp. 292–303 in *Applied algebra, algebraic algorithms and error-correcting codes* (Tokyo, 1980), edited by S. Sakata, Lect. Notes in Comput. Sci. **508**, Springer, 1991. MR Zbl

[Schmidt-Göttsch 1989] K. Schmidt-Göttsch, "Polynomial bounds in polynomial rings over fields", *J. Algebra* **125**:1 (1989), 164–180. MR Zbl

[Schoutens 2010] H. Schoutens, *The use of ultraproducts in commutative algebra*, Lecture Notes in Math. **1999**, Springer, 2010. MR Zbl

[Seidenberg 1974] A. Seidenberg, "Constructions in algebra", *Trans. Amer. Math. Soc.* **197** (1974), 273–313. MR Zbl

[Simmons and Towsner 2019] W. Simmons and H. Towsner, "Proof mining and effective bounds in differential polynomial rings", *Adv. Math.* **343** (2019), 567–623. MR Zbl

[Stanley 1986] R. P. Stanley, *Enumerative combinatorics, I*, Wadsworth & Brooks/Cole, Monterey, CA, 1986. MR Zbl

[Towsner 2018] H. Towsner, "What do ultraproducts remember about the original structures?", preprint, 2018. arXiv

[van der Waerden 1970] B. L. van der Waerden, *Algebra, I*, Ungar, New York, 1970. MR

Received June 7, 2019. Revised January 28, 2020.

WILLIAM SIMMONS
DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
HOBART AND WILLIAM SMITH COLLEGES
GENEVA, NY
UNITED STATES

wsimmons@hws.edu

HENRY TOWSNER
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF PENNSYLVANIA
PHILADELPHIA, PA
UNITED STATES

htowsner@math.upenn.edu

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2020 is US $520/year for the electronic version, and $705/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 306 No. 2 June 2020