Absolute Primality of Polynomials is Decidable in Random Polynomial Time in the Number of Variables

Joos Heintz and Malte Sieveking

Abstract. Let F be a n-variate polynomial with $\deg F = d$ over an infinite field k_0. Absolute primality of F can be decided randomly in time polynomial in n and exponential in d^5 and determinalistically in time exponential in $d^6 + n^2 d^3$.

Let $k_0 \subset k$ fields, k being algebraically closed.
We call a polynomial $F \in k_0[X_1,..,X_n]$ in the indeterminates $X_1,...,X_n$ over k_0 absolutely prime, if F is prime over k. With other words: F is absolutely prime if F is prime considered as an element of $k[X_1,..,X_n]$. We remark that the notion of absolute primality doesn't depend on the specific algebraically closed extension of k_0 we have chosen. For example, $F \in \mathbb{Q}[X_1,..,X_n]$ is absolutely prime iff it is prime over $\mathbb{C}$. ($\mathbb{Q}$ denotes as usual the rational and $\mathbb{C}$ the complex numbers.)

If $n = 1$ the absolutely prime polynomials are exactly the linear ones. For $n \geq 2$ there is no chance of such a general and simple description of the absolutely prime polynomials over given ground field k_0, even if k_0 is algebraically closed. (This would solve the problem of classifying algebraic varieties up to birational equivalence.)
However, if we can effectively perform arithmetic operations in k, we can decide whether a given polynomial over k is absolutely prime or not, since we have algorithms for quantifier elimination in the first order theory of k. For given polynomial $F \in k_0[X_1,..,X_n]$ with degree $\deg F = d$ we write up a first order formula in the coefficients of F which says that F has no factor of degree $0 < d' < d$.
Such a formula contains $b \cdot \frac{(n+d)^n}{(n-1)!}$ bounded variables and as much quadratic polynomials, where $b > 0$ is some constant. The best known quantifier elimination algorithms for algebraically closed fields are polynomial in degree and number of polynomials appearing in the formula but hyperexponential in the number of variables. (Compare [5]). If we apply such an algorithm to our problem to decide whether F is absolutely prime or not, we need $O(2^{2^{\frac{(n+d)^{Bn}}{(n-1)!}}})$ steps to get a quantifier free formula in the coefficients of F which is true iff F is absolutely prime, for $B > 0$

some constant. Even if verifying polynomial identities in k_0 is free, this straight forward algorithm has a complexity which is hyperexponential in degree and triple exponential in the number of variables.

Our main result can be stated as follows :

Theorem 1 : Let k_0 be an infinite field. Then there exist constants $C > 0$ and $c > 0$ such that absolute primality of any multivariate polynomial F over k_0 can be decided randomly

$$\text{in} \quad C\, n^d\, 2^{c d^5} \quad \text{arithmetical steps (the operations: +,*,/)}$$

where n is the number of indeterminates appearing in F and $d = \deg F$.

The deterministic bound for the decision procedure is

$$C_1\, 2^{c_1 (d^6 + n^2 d^3)}$$

for some constants $C_1 > 0$, $c_1 > 0$.

In the case of $k_0 = \mathbb{Q}$ we have an encoding of the elements of k_0 on a Turing Machine tape such that the arithmetical operations of k_0 can be performed in time quadratic in the length of the input.

In this case the Turing complexity of the random procedure is bounded by

$$C_2\, n^{2d}\, 2^{c_2 d^5 \sigma(F)^2}$$

where $\sigma(F)$ denotes the maximal length of the coefficients of F in the encoding, and $C_2 > 0$, $c_2 > 0$ are some constants.

The deterministic Turing complexity of our procedure is bounded by

$$C_3\, 2^{c_3 (d^6 + n^2 d^3)\, \sigma(F)^2}$$

for suitable $C_3 > 0$, $c_3 > 0$.

If $\operatorname{char} k_0 = p > 0$ and if k_0 is the algebraic closure of its prime field $\mathbb{Z}_p$, similar results hold with $\sigma(F) := (\deg F)^5$.

The assumption for k_0 to be infinite is not essential. In fact, our decision procedure works for any coefficient field k_0 and for any polynomial F over k_0 provided that $\# k_0 \geq C_4\, 2^{c_4 (\deg F)^5}$ for some universal constants $C_4 > 0$, $c_4 > 0$. So, working in a finite extension of k_0 , if necessary, we can apply our decision procedure also to the case of k_0 to be finite.

Our methods don't depend on the charakteristic of k_0 . So, for the sake of simplicity, we shall restrict ourselves to the case $k_0 = \mathbb{Q}$.

We need some algebraic geometry. Terminology and prerequisites are given for example in [1] and [4] or can be found (with exception of the Bezout inequality [1],[2]) in any standard text book about classical algebraic geometry, for instance [9] or [7] .

Furthermore, we need a General Hyperplane Section Lemma, which we state in the following form :

Lemma 2 : Let k be algebraically closed and $X_1,\ldots,X_n$ indeterminates over k . Let p be a prime ideal of $k[X_1,..,X_n]$ which defines an affine subvariety of k^n of dimension $r \geq 2$. Let A_{ij}, A_i , $i = 1,..,r-1$, $j = 1,..,n$ be transcendent quantities over k , and let K be an algebraically closed field containing k and A_{ij}, A_i , $i = 1,..,r-1$, $j = 1,..,n$.

Then the ideal $p + (X_1 - \sum_{1<j} A_{1j} X_j - A_1 , \ldots, X_{r-1} - \sum_{r-1<j} A_{r-1\,j} X_j - A_{r-1})$ is prime in $K[X_1,..,X_n]$.

We apply Lemma 2 in the case $k = \mathbb{C}$ and $p = (F)$, where $F \in \mathbb{Q}[X_1,..,X_n]$ with $n \geq 2$ and $\deg F = d$ is the polynomial from which we want to decide if it is absolutely prime or not. In this case $r = n-1$.

Let R be the polynomial ring generated over $\mathbb{Q}$ by A_{ij}, A_i , $i = 1,..,n-2$, $j = 1,..,n$, L the fraction field of R , and K be an algebraically closed field containing L and $\mathbb{C}$.

Let $\varphi : \mathbb{Q}[X_1,..,X_n] \longrightarrow R[X_{n-1},X_n]$ be the $\mathbb{Q}$-algebra homomorphism obtained by successively substituting X_i by $\sum_{j>i} A_{ij} X_j + A_i$.

Then (F) and $(F) + (X_1 - \sum_{j>1} A_{1j} X_j + A_1 , \ldots, X_{n-2} - \sum_{j>n-2} A_{n-2\,j} X_j - A_{n-2})$ have the same image (F^*) , where $F^* \in R[X_{n-1},X_n]$ with $\deg F^* = d$. Note that the coefficients of F^* are polynomials in A_{ij}, A_i , $i = 1,..,n-2$, $j = 1,..,n$ of degree $\leq d$. Furthermore, if the degree of F in X_n , $\deg_{X_n} F = \deg F$, then $\deg_{X_n} F^* = \deg F^*$, and the leading coefficient of X_n in F^* is in $\mathbb{Q}$.

Now we extend φ to a $\mathbb{C}$-algebra homomorphism $\mathbb{C}[X_1,..,X_n] \longrightarrow K[X_{n-1},X_n]$.

By the General Hyperplane Section Lemma,

F prime in $\mathbb{C}[X_1,..,X_n]$ implies F^* prime in $K[X_{n-1},X_n]$.

Obviously, F reducible in $\mathbb{C}[X_1,..,X_n]$ implies F^* reducible in $K[X_{n-1},X_n]$.

So we have finally :

F absolutely prime iff F* absolutely prime.

Since $k_0 = \mathbb{Q}$ is infinite, we may, after a suitable linear transformation of $X_1,\dots,X_n$, assume that $\deg F = \deg_{X_n} F$.

So far, we have reduced the problem of deciding absolute primality of F to the case of deciding absolute primality of some other polynomial F* in only the two variables X_{n-1}, X_n over some extension field L of $\mathbb{Q}$. We have $\deg F^* = \deg F = d$, and we may assume $\deg_{X_n} F^* = d$, the leading coefficient of X_n in F* being 1, if $d > 0$. Furthermore, we keep in mind that the coefficients of F* are polynomials in $\leq n(n-2)$ indeterminates over $\mathbb{Q}$.

In the sequel let L be any field containing $k_0 = \mathbb{Q}$, X,Y indeterminates over L, K the algebraic closure of L, and $F \in K[X,Y]$, with $d = \deg F = \deg_Y F > 0$. Let $m = d^2$ and $x_1,\dots,x_m$ m different numbers of $\mathbb{Q}$, for example $1,\dots,d^2$.

Lemma 3 : F is reducible over K iff there exist $0 < d' < d$ and $y_{11},\dots,y_{1d'},\dots,y_{m1},\dots,y_{md'} \in K$ such that

$$F(x_i, y_{ij}) = 0 \quad \text{for } i = 1,\dots,m,\ j = 1,\dots,d'$$

and such that the inhomogeneous linear equation system

$$(*) \qquad \begin{aligned} \sum_{k \leq d'-1} G_{kl}\, x_i^k &= (-1)^l \sigma_l(y_{i1},\dots,y_{id'}) \qquad l = 1,\dots,d',\ i = 1,\dots,m \\ G_{0d'} &= 1 \end{aligned}$$

in the unknowns G_{kl}, $k = 0,\dots,d'$, $l = 0,\dots,d'$, $k+l \leq d'$ has a solution in $K^{\binom{d'+1}{d'-1}}$. σ_j denotes the j-th elementary symmetric polynomial in d' variables.

Proof : If F is reducible over K, let G be a factor of F with $0 < d' = \deg G < d$. Since $\deg_Y F = \deg F$ we have $\deg_Y G = \deg G > 0$, and we may assume that the leading coefficient of Y in G is 1.

Let $G = \sum_{\substack{0 \leq k,l \leq d' \\ k+d \leq d'}} g_{kl} X^k Y^l$.

Since K is algebraically closed and the leading coefficient of Y in each $G(x_i,Y)$ is 1, we can choose for each $i = 1,\dots,m$ $y_{i1},\dots,y_{id'}$ such that

$$G(x_i, Y) = \prod_{1 \le j \le d'} (Y - y_{ij}) .$$

Then we have for each $l = 1,\ldots,d'$

$$\sum_{k \le d'-l} g_{kl} x_i^k = (-1)^l \sigma_l(y_{i1},\ldots,y_{id'}) \quad \text{and} \quad g_{0d'} = 1 ,$$

so (*) has a solution and $F(x_i,y_{ij}) = 0$ for $i = 1,..,m$, $j = 1,..,d'$.

Now suppose F prime over K. If there exist $0 < d' < d$ and $y_{11},\ldots,y_{1d'},\ldots,y_{m1},\ldots,y_{md'}$ such that $F(x_i,y_{ij}) = 0$ for $i = 1,\ldots,m$, $j = 1,\ldots,d'$ and such that (*) has a solution $(g_{kl})_{\substack{0 \le k,l \le d' \\ k+l \le d'}}$ in $K^{\binom{d'+1}{d'-1}}$, let

$$G := \sum_{\substack{0 \le k,l \le d' \\ k+l \le d'}} g_{kl} X^k Y^l \in K[X,Y] .$$

Clearly, $\deg G = d'$ and $G(x_i,y_{i1}) = 0$ for $i = 1,..,m$. So $\#\{F=0\} \cap \{G=0\} \ge m = d^2$ since the $(x_1,y_{11}), \ldots, (x_m,y_{m1})$ are all different common zeroes of F and G . On the other side G is not a multiple of F, since $\deg G = d' < d = \deg F$. So, by the Dimension Theorem, $\#\{F=0\} \cap \{G=0\} < \infty$, since F is prime. Then, by the Bezout Inequality [1] follows $\#\{F=0\} \cap \{G=0\} \le \deg F \cdot \deg G = d\,d' < d^2$, a contradiction.

The entries of the matrix of (*) are in $\mathbb{Q}$ and only dependent on the choice of $x_1,\ldots,x_m$. Applying Gauss elimination we can exprime the solvability of (*) saying that some $\le d^2 = m$ $\mathbb{Q}$-linear combinations of the set $\{1\} \cup \{\sigma_l(y_{i1},\ldots,y_{id'}) ; l = 1,..,d' , i = 1,..,m\}$ have to be 0 .

Given $x_1,\ldots,x_m \in \mathbb{Q}$ we can compute the coefficients of these linear combinations in $O(d^{12})$ arithmetical steps.

With these preparations we have the following corollary of Lemma 3 :
Let Y_{ij} , $i = 1,\ldots,m$, $j = 1,\ldots,d-1$, new indeterminates over K .

Corollary 4 : Given $F \in L[X,Y]$ with $d = \deg F = \deg_Y F > 0$ and given $m = d^2$ different numbers $x_1,\ldots,x_m \in \mathbb{Q}$.
With $O(2^{c\,d})$ arithmetical steps (where $c > 0$ is some constant) there can be computed the coefficients of polynomials

$$H_{11},..,H_{m1} \in \mathbb{Q}[Y_{11},..,Y_{m1}] , \ldots , H_{1d-1},..,H_{md-1} \in \mathbb{Q}[Y_{11},..,Y_{1d-1},\ldots,Y_{m1},..,Y_{md-1}]$$

of degree $\le d$, with the following property :

F is reducible over K iff there exists $0 < d' < d$ such that the ideal generated by $\{F(x_i,Y_{ij}) ; i = 1,..,m , j = 1,..,d'\} \cup \{H_{id'}(Y_{11},..,Y_{md'}) ; i = 1,..,m\}$ in $L[Y_{11},..,Y_{md'}]$ has a zero in $K^{md'}$.

Corollary 4 is nothing but a reformulation of Lemma 3, avoiding algebraic elements over L . We omit its proof.
For given $0 < d' < d$ the $H_{1d'},\ldots,H_{md'}$ are linear combinations over $\mathbb{Q}$ of 1 and the d'-variate elementary symmetric polynomials in the variable sets $\{Y_{11},..,Y_{1d'}\},\ldots,\{Y_{m1},..,Y_{md'}\}$. $H_{11},\ldots,H_{md-1}$ can be chosen uniformly for all $F \in L[X,Y]$ with $d = \deg F = \deg_Y F > 0$.

Let $0 < d' < d$. Put $r = m\,d'$ and give the elements of $\{(i,j) : i=1,..,m , j=1,..,d'\}$ numbers $s = 1,\ldots,r$.
For s, the number of (i,j) , write $Y_s := Y_{ij}$, $F_s(Y_s) := F(x_i,Y_{ij})$ and $H_s(Y_1,..,Y_s) := H_{ij}$. Note that $\deg F_s = d$, and that the leading coefficient of F_s, $s=1,..,r$, is 1 .
Let $U_1,\ldots,U_r$ be new indeterminates over K , and let $\tilde{K}$ be the algebraical closure of $K(U_1,..,U_r)$.
Since for each $s=1,\ldots,r$ F_s is a polynomial of degree $d>0$ in only the indeterminate Y_s , the following equivalence holds :

the ideal generated by

$$\{ F_s ; s = 1,\ldots,r \} \cup \{ H_s ; s = 1,\ldots,r \}$$

in $L[Y_1,..,Y_r]$ has a zero in K^r iff
the ideal generated by

$$\{ F_s ; s = 1,\ldots,r \} \cup \{ U_1 H_1 + \ldots + U_r H_r \}$$

in $L(U_1,..,U_r)[Y_1,..,Y_r]$ has a zero in $\tilde{K}^r$.

Now we are ready to work with resultants.
We define a sequence $R_r,\ldots,R_0$ of polynomials with $R_s \in L[U_1,..,U_r , Y_1,..,Y_s]$ for $s=1,\ldots,r$ and $R_0 \in L[U_1,..,U_r]$ such that the following holds :

the ideal generated by $\{F_s ; s=1,..,r\} \cup \{U_1 H_1 + \ldots + U_r H_r\}$ in $L(U_1,\ldots,U_r)[Y_1,..,Y_r]$ has a zero in $\tilde{K}^r$ iff $R_0 = 0$.

The construction of $R_r, \ldots, R_0$:

Put $R_r := U_1 H_1 + \ldots + U_r H_r$.

For $s = 1,\ldots,r-1$ let $R_{s+1} \in L[U_1,..,U_r,Y_1,\ldots,Y_{s+1}]$ be already constructed.
Let D be the resultant of R_{s+1} und F_{s+1} (eliminating Y_{s+1}).
Then $D \in L[U_1,..,U_r,Y_1,..,Y_s]$. Since $F_1,..,F_s$ are 1-variate polynomials in the indeterminates $Y_1,..,Y_s$ respectively, division with remainder by $F_1,..,F_s$ is defined in $L[U_1,..,U_r,Y_1,..,Y_s]$. Now divide D by F_1 , then its remainder by F_2 and continue this procedure for $F_3,..,F_s$. We define R_s to be the polynomial finally obtained in this way. $R_s - D$ is in the ideal generated by $F_1,\ldots,F_s$ in $L[U_1,..,U_r,Y_1,..,Y_s]$.
Furthermore, we have $\deg_{Y_1} R_s, \ldots, \deg_{Y_s} R_s < d$
Finally we put R_0 to be the resultant of R_1 und F_1 .
Since $\deg F_1 = \ldots = \deg F_s = d > 0$ one sees inductively : The ideal generated by $\{F_s ; s = 1,..,r\} \cup \{U_1 H_1 + \ldots + U_r H_r\}$ in $L(U_1,..,U_r)[Y_1,..,Y_r]$ has a zero in $\tilde{K}^r$ iff $R_0 = 0$.

Note for later application, that, if the coefficients of F are $n(n-2)$-variate polynomials over $\mathbb{Q}$ of degree $\leq d$, then R_0 is a $n(n-2)+r$-variate polynomial over $\mathbb{Q}$ of degree $O(d^{2d^2})$.

$R_r,..,R_0$ are defined by an algorithm. To compute R_0 we have to perform $O(d^{12\,d^4})$ arithmetical operations in $L(U_1,..U_r)$.
Note that the sequence $R_r,..,R_0$ depends on F and $0 < d' < d$. So let us write $r^F_{d'} := R_0$.

Putting together all our material, the following proposition is self explanatory :

Proposition 5 : Let $U_1,U_2,\ldots$ be indeterminates over L . There is a constant $c > 0$ such that for each $F \in L[X,Y]$ with $d = \deg F = \deg_Y F$ there can be computed $d-1$ quantities $r^F_1,\ldots, r^F_{d-1} \in L[U_1,..,U_{d^3}]$ with $O(2^{c\,d^5})$ arithmetical operations over $L(U_1,..,U_{d^3})$ such that the following holds :

$$F \text{ absolutely prime} \iff r^F_1 \neq 0 , \ldots , r^F_{d-1} \neq 0 .$$

Now we turn back to the situation we started from.

Let $F \in \mathbb{Q}[X_1,..,X_n]$. We want to decide the absolute primality of F . Without loss of generality we may assume $n \geq 2$ and $d = \deg F > 0$. By a linear transformation of $X_1,...,X_n$ which costs at most $O(n^d)$ arithmetical operations in $\mathbb{Q}$ we may furthermore assume $\deg F = \deg_{X_n} F$. Let A_{ij} , A_i , $i = 1,..,n-2$, $j = 1,..,n$ and $U_1,...,U_d$ be indeterminates over $\mathbb{C}$, let R the polynomial ring generated over $\mathbb{Q}$ by A_{ij} , A_i , $i = 1,...,n-2$, $j = 1,...,n$, L the fraction field of R and $F^* \in R[X_{n-1}, X_n]$ as at the beginning. We have $d = \deg F^* = \deg_{X_n} F^*$, and we may assume that the leading coefficient of X_n in F^* is 1 .

To F^* we can apply Proposition 5. We have $r_1^{F^*},...,r_{d-1}^{F^*} \in R[U_1,..,U_{d^3}]$ and $\deg r_1^{F^*},...,\deg r_{d-1}^{F^*} \leq C_0\, d^{2\,d^2}$ and $r_1^{F^*},...,r_{d-1}^{F^*}$ can be computed in $L(U_1,..,U_r)$ with $C_1\, 2^{c_1 d^5}$ arithmetical operations, where $C_0 > 0$, $C_1 > 0$ and $c_1 > 0$ are constants not depending on F . Furthermore, we have :

$$F \text{ absolutely prime} \quad \text{iff} \quad r_1^{F^*} \neq 0\,,\ \ldots,\ r_{d-1}^{F^*} \neq 0 \quad .$$

Let $N := (n-2)n + d^3$. $r_1^{F^*},...,r_{d-1}^{F^*}$ are N-variate polynomials over $\mathbb{Q}$ which we interprete as functions on $\mathbb{Q}^N$. Going back to the construction of $r_1^{F^*},...,r_{d-1}^{F^*}$ by resultants, we see that we can evaluate $r_1^{F^*},...,r_{d-1}^{F^*}$ at any $z \in \mathbb{Q}^N$ in $C_3\, n^d\, 2^{c_3 d^5}$ arithmetical steps, where $C_3 > 0$ and $c_3 > 0$ are constants. Since $r_1^{F^*},...,r_{d-1}^{F^*}$ have degree $\leq C_0\, d^{2\,d^2}$ we have to evaluate them at $(C_0\, d^{2d^2})^N$ points of $\mathbb{Q}^N$ to check whether they all are different from 0 or not.

This gives the deterministic bound stated in Theorem 1 for the problem to decide absolute primality of F , namely

$$O\left(\, 2^{c_4 (\, d^6 + n^2\, d^3)}\,\right) \quad \text{for some} \quad c_4 > 0 \quad .$$

In order to get the probabilistic bound of Theorem 1 , we apply [4] , Theorem 4.4 .

Let $v := \lceil\, 2\, C_1\, 2^{c_1 d^5}\, (\, C_0 d^{2\, d^2} + 1)^2 \,\rceil$ and

$q := \lceil\, 6\, (\, C_1\, 2^{c_1 d^5} + 1)(\, C_1\, 2^{c_1 d^5} + 2)\,\rceil$ where

$\lceil\ \rceil$ denotes the least upper integer bound.

We have $v, q \leq C_4\, 2^{c_4\, d^5}$ for some $C_4 > 0$, $c_4 > 0$.

Let $[v] = \{1,\ldots,v\}$. Then by [4] , Theorem 4.4 any randomly chosen sequence $z_1,\ldots, z_q \in [v]^N \subset \mathbb{Q}^N$ is with probability $\geq 1 - v^{-\frac{q}{6}} > \frac{1}{2}$ a correct test sequence for the complexity class of $r_1^{F^*},\ldots,r_{d-1}^{F^*}$. With other words : The probability that $r_1^{F^*} \neq 0,\ldots, r_{d-1}^{F^*} \neq 0$ but for some $i=1,\ldots,d-1$ $r_i^{F^*}(z_1) = 0,\ldots, r_i^{F^*}(z_q) = 0$ is $\leq v^{-\frac{q}{6}} < \frac{1}{2}$.

To compute $r_1^{F^*}(z_1),\ldots, r_1^{F^*}(z_q),\ldots, r_{d-1}^{F^*}(z_1),\ldots, r_{d-1}^{F^*}(z_q)$ we need $C_5 n^d 2^{c_5 d^5}$ arithmetical steps, $C_5 > 0$, $c_5 > 0$ being constants.

To decide absolute primality of F choose randomly a sequence $z_1,\ldots,z_q \in [v]^N$ and check if for any $i=1,\ldots,d-1$ there is a $j=1,\ldots,q$ such that $r_i^{F^*}(z_j) \neq 0$. If this is the case, decide F to be absolutely prime, otherwise that F is reducible over $\mathbb{C}$.

This is a random algorithm for deciding absolute primality of F working in $C_5 n^d 2^{c_5 d^5}$ arithmetical steps as stated in Theorem 1 .

The Turing complexity bounds of Theorem 1 are straight forward by analyzing the algorithms step by step and verifying that the length of the numbers involved doesn't grow too much.

Remarks to the proof of Theorem 1 :

The use of the Bezout-Inequality in the case of $n=2$ can be avoided by using resultants. But then, the proof, thus elementarized, is less elegant and gives slightly worse bounds. This elementarized proof can easily be generalized to arbitrary $n \geq 2$. But then, the bounds become hyperexponential in n . The great advantage of using the General Hyperplane Section Lemma is that the bounds become polynomial in n in the random case and simply exponential in n in the deterministic case.

Finally we are going to say some words about the connection of Theorem 1 with the problem to decide whether a given set of polynomials defines an irreducible algebraic set.
For the sake of simplicity assume $k_0 = k$ algebraically closed.

Let $X_1,\ldots,X_n$ indeterminates over k .

Let $F_1,\ldots,F_m \in k[X_1,..,X_n]$ and $d := \sum_{1\le k\le m} \deg F_k$.

Let $V := \{F_1 = 0 ,\ldots, F_m = 0\}$, the set of common zeroes of $F_1,\ldots,F_m$ in k^n .

For given $F_1,\ldots,F_m$ we want to decide whether V is irreducible or not.

As in [1] , [2] , define $\deg V := \sum_{C \text{ component of } V} \deg C$.

By [2] , Corollary 1 , [1] , Corollary 2 respectively, we have $\deg V \le (1+d)^n$.

Let $r := \max_{C \text{ component of } V} \dim C$ as in [4] .

If r is known , we can use Theorem 1 to decide the irreducibility of V :

As a consequence of [2] , Lemma 1 and the proof of Lemma 3 there is a Zariski open set of $k^{n(r+1)}$ of linear maps $k^n \to k^{r+1}$ mapping V on a reducible r-dimensional subset of k^{r+1} if V itself is reducible and on a r-dimensional irreducible subset of k^{r+1} if V is irreducible. By [2] , Lemma 2 the degree of the image of V is $\le (1+d)^n$.

This geometric fact can be translated into the language of formal manipulations :

Choose new indeterminates A_{ij} , $i = 1,\ldots,r+1$, $j = 1,\ldots,n$ and $Y_1,\ldots,Y_{r+1}$ over k .
Let L be the field generated by A_{ij} , $i = 1,\ldots,r+1$, $j = 1,\ldots,n$ over k .
Consider $(F_1,..,F_m)$ as an ideal in $L[X_1,..,X_n]$.

Compute $G(Y_1,\ldots,Y_{r+1}) \in L[Y_1,\ldots,Y_{r+1}]$ with

$$G\Big(\sum_{1\le j\le n} A_{1j} X_j ,\ldots, \sum_{1\le j\le n} A_{r+1\,j} X_j\Big) \in (F_1,\ldots,F_m) \ , \ G \neq 0$$

and $\deg G$ minimal. By [6] or [10] , Prop. 1 and the fact that $\deg V \le (1+d)^n$, this is possible in $O(d^{2^{c\,n^2}})$ arithmetical operations in k , where $c > 0$ is some constant. G is not a unit in $L[Y_1,..,Y_{r+1}]$ and $\deg G \le (1+d)^n$.

So without loss of generality, we may assume $\deg_{Y_1} G > 0$.

Let $D :=$ greatest common divisor of G and $\frac{\partial G}{\partial Y_1}$ and $F := \frac{G}{D}$ in $L[Y_1,..,Y_{r+1}]$.

We have $\deg F \le (1+d)^n$ and F can be computed in $O(d^{2^{c\,n^2}})$ arithmetical steps in k .

By our geometric fact it is easily seen that

$$F \in L[Y_1,..,Y_{r+1}] \text{ absolutely prime iff } V \text{ irreducible.}$$

So we get for some $c_1 > 1$ a deterministic $O(2^{d^{c_1 n^2}})$ - bound for the problem to decide the irreducibility of $V = \{F_1 = 0, \ldots, F_m = 0\}$, where $F_1, \ldots, F_m \in k[X_1, \ldots, X_n]$ and $d = \sum_{1 \leq k \leq m} \deg F_k$, if $r = \dim V$ is known.

This bound is much better than the bound obtained by converting the problem into a first order formula and applying then quantifier elimination, however, it is still hyperexponential in n.

The restriction that r has to be known is not essential if we accept bounds hyperexponential in n. In fact, by [5] r can be computed in $O(d^{2^{c_2 n^2}})$ steps, where $c_2 > 0$ is some suitable constant.

Putting this result together with the result presented in [3], we have for some $c_3 > 0$, $c_4 > 0$ a deterministic $O(d^{2^{2^{c_3 n^2}}} + 2^{d^{c_4 n^2}})$ - procedure to decide

$$(F_1, \ldots, F_m) \text{ prime in } k[X_1, \ldots, X_n] \text{ and } V := \{F_1 = 0, \ldots, F_m = 0\} \text{ smooth.}$$

This bound is very bad in n but still simply exponential in d. In any case it is much better than bounds obtained by applying general quantifier elimination.

Appendix

We prove the General Hyperplane Section Lemma (Lemma 2) modulo [8], Chapter VIII § 6 Lemma.

Let k be an algebraically closed field, $S = k[\pi_1, \ldots, \pi_n]$ the coordinate ring of some (irreducible) affine k-variety of dimension $r \geq 2$.
Let A_{ij}, A_i, $i = 1, \ldots, r-1$, $j = 1, \ldots, n$ be indeterminates over S, R the ring generated by A_{ij}, A_i, $i = 1, \ldots, r-1$, $j = 1, \ldots, n$ over k, L the fraction field of R, and K the algebraic closure of L. Let

$$H_i := \pi_i - \sum_{i<j} A_{ij} \pi_j - A_i \in R \otimes_k S, \quad i = 1, \ldots, r-1,$$

and write $T := R \otimes_k S / (H_1, \ldots, H_{r-1})$.

$(H_1, \ldots, H_{r-1})$ is the kernel of the homomorphism $R \otimes_k S \to R \otimes_k S$ which maps A_i on $\pi_i - \sum_{i<j} A_{ij} \pi_j$, $i = 1, \ldots, r-1$. $R \otimes_k S$, being a polynomial ring over S has no zero divisors, hence T as a subring of $R \otimes_k S$ is an integral domain.

Let Q be the fraction field of T.

By the methods used in [2], Lemma 1 it can easily be seen that R is a subring of T, hence L is contained in Q. From [8], Chapter VIII §6 Lemma it follows that L is algebraically closed in Q. We are going to show that $K \otimes_R T$ is an integral domain.

Let L_{sep} be the separable closure of L in K. We first show that $L_{sep} \otimes_R T$ is integral. If not, let $\xi \in L_{sep}$ such that $L(\xi) \otimes_R T$ contains zero divisors.

Let X be an indeterminate over Q and let $F(X) \in L[X]$ be the minimal polynomial of ξ over L. Since $L(\xi) \otimes_R T = (L \otimes_R T)[\xi]$ contains zero divisors, F is not irreducible considered as polynomial over Q.

Let G be a factor of F in $Q[X]$ with $\deg F > \deg G > 0$ and leading coefficient 1. The coefficients of G are algebraic over L and are in Q. Since L is algebraically closed in Q, they are in L. So G is a factor of F in $L[X]$, which is impossible since F is irreducible over L and $0 < \deg G < \deg F$.
So our claim is shown in the case $\operatorname{char} k = 0$.

Now suppose $\operatorname{char} k = p > 0$. If $K \otimes_R T$ is not integral, then there are $z_1, z_2 \in K \otimes_R T$ different from 0 such that $z_1 z_2 = 0$. There exists a natural number f such that $z_1^{p^f}, z_2^{p^f} \in Q_{sep}$, the fraction field of $L_{sep} \otimes_R T$. So we may assume $z_1^{p^f} = 0$. But then $z_1 \in Q_{sep} \subset K \otimes_R T$, whence $z_1 = 0$. Contradiction.

Now let $X_1, \ldots, X_n$ be indeterminates over k, $p \subset k[X_1, \ldots, X_n]$ a prime ideal defining a variety of dimension $r \geq 2$, and A_{ij}, A_i, $i = 1, \ldots, r-1$, $j = 1, \ldots, n$, as in Lemma 1.
Put $S = k[X_1, \ldots, X_n]/p$. Now the General Hyperplane Section Lemma (Lemma 2) follows.

References

[1] Heintz, J. : Definability Bounds of First Order Theories of Algebraically Closed Fields (Abstract). Proc. Fundamentals of Computation Theory FCT'79 (1979), p. 160-166 .

[2] " : " (1977) (unpublished).

[3] " : Towards a Decision Procedure for Prime Ideals in Polynomial Rings. Report on the 1979 Oberwolfach Conference on Complexity Theory, (1979) .

[4] " , Schnorr, C.P. : Testing Polynomials which are Easy to Compute. 12 th Annual Symp. ACM on Computing, (1980), p. 262-272 .

[5] " , Wüthrich, R. : An Efficient Quantifier Elimination Algorithm for Algebraically Closed Fields of Any Characteristic. SIGSAM Bull. Vol. 9 , No 4 , (1975), p. 11.

[6] Herrmann, G. : Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. 95 (1926), p. 736-788 .

[7] Kendig, K. : Elementary Algebraic Geometry. New York, Springer Verlag, (1970) .

[8] Lang, S. : Introduction to Algebraic Geometry. New York, Interscience, (1964) .

[9] Šafarevič, I.R. : Osnovy Algebraičeskoj Geometrii. Moskva, Nauka, (1972) . English Translation: Basic Algebraic Geometry. Springer Verlag, (1974) .

[10] Seidenberg, A. : Constructions in Algebra. Trans. AMS, Vol. 194, (1974), p. 273-313 .

Incognito ergo sum.