INDECOMPOSABILITY OF POLYNOMIALS VIA JACOBIAN MATRIX

GUILLAUME CHÈZE AND SALAH NAJIB

Abstract. Indecomposable polynomials are a special class of absolutely irreducible polynomials. Some improvements of important effective results on absolute irreducibility have recently appeared using Ruppert's matrix. In a similar way, we show in this paper that the use of a Jacobian matrix gives sharp bounds for the indecomposability problem.

1. Introduction

Let $n \geq 2$ be an integer and $\underline{X} = (X_1, \dots, X_n)$ be a $n-$tuple of variables. In this article, we use the following definition of decomposable polynomials: a non-constant polynomial $f(\underline{X}) \in \mathbb{K}[\underline{X}]$ with coefficients in a field $\mathbb{K}$ is decomposable over $\mathbb{K}$ if there exist polynomials $h(\underline{X}) \in \mathbb{K}[\underline{X}]$ and $u(T) \in \mathbb{K}[T]$ with $\deg(u) \geq 2$ such that $f(\underline{X}) = u\big(h(\underline{X})\big)$. Otherwise, f is said to be indecomposable.

It is known that a decomposable polynomial is absolutely reducible (i.e., reducible in $\overline{\mathbb{K}}[\underline{X}]$ where $\overline{\mathbb{K}}$ is an algebraic closure of $\mathbb{K}$). Indeed, if $f = u \circ h$ then $f = \prod_i (h - u_i)$ where $u_i \in \overline{\mathbb{K}}$ are the roots of u. Some authors (see, e.g., [21, 8, 16]) study the behavior of the absolute factorization after some perturbations: reduction modulo p, reduction from n to 2 variables. The key point is that these problems can be reduced to linear algebra. The matrix used for the absolute factorization is derived from the computation of the first algebraic de Rham cohomology group of the complement of a plane curve (see the description of Ruppert's and Gao's algorithms in [4, Related Works], [17, page 4] or [22]). This matrix is the so-called Ruppert's matrix (see [21], [23, chapter 3]). In this paper, we show that the indecomposability of a polynomial f can also be reduced to a linear algebra problem. We introduce a special matrix derived from an algebraic dependence relation, which we call the *Jacobian matrix* and denote by Jac_f. Using this matrix, we construct bounds for the indecomposability problem.

In Section 2, we recall some classical results about indecomposability and the Jacobian matrix. These results are well-known in characteristic zero. In this section, we extend them to positive characteristic. Then, in order that this paper be self-contained, we show that the "usual proof" also works in a more general context. These results state that the indecomposability problem can be solved using only linear algebra.
Section 3 is devoted to some analogs of well-known absolute irreducibility theorems in our indecomposability context. More precisely, we show how the study of a multivariate polynomial can be restricted to the study of a bivariate polynomial. Then,

we show that the set of decomposable polynomials is included in an algebraic variety, and we give a bound for the degree of our *Noether's indecomposability forms* (see Theorem 9). These results on absolute irreducibility are called Bertini's and Noether's theorems (see, e.g., [7, 15, 16, 17, 21], and [23, chapter 3]). Moreover, at the end of Section 3, we investigate the specialization of indecomposable polynomials.
In Section 4, we study the reduction modulo p of an indecomposable polynomial with integer coefficients. We show that if p is a large enough prime, then f is indecomposable implies that $f \mod p$ is indecomposable.
Finally, in Section 5, we use a property of Newton's polygons to produce an indecomposability test. Some computation times are given in order to show the practical behavior of this test.

2. Jacobian derivation and decomposable polynomials

Notations: The following notations will be retained throughout the article:
We denote by $\mathbb{K}$ an arbitrary field of characteristic $p \geq 0$.
For an integer $n \geq 2$, we denote by $\underline{X} = (X_1, \dots, X_n)$ an $n-$tuple of algebraically independent variables (over $\mathbb{K}$).
We sometimes write $f = u \circ h$ instead of $f(\underline{X}) = u(h(\underline{X}))$.
We denote by $\deg(f)$ the total degree of f.
We denote by $\partial_X f$ the partial derivative of f with respect to X.
Given a field $\mathbb{F}$, we denote by $\overline{\mathbb{F}}$ an algebraic closure of $\mathbb{F}$.

2.1. **Algebraic dependence and the Jacobian.**
In this section, we present our basic toolbox.

Definition 1. Let $f(\underline{X}) \in \mathbb{K}[\underline{X}]$ be a non-constant polynomial. The polynomial f is said to be decomposable over $\mathbb{K}$ if there exist polynomials $h(\underline{X}) \in \mathbb{K}[\underline{X}]$ and $u(T) \in \mathbb{K}[T]$ with $\deg(u) \geq 2$ such that $f(\underline{X}) = u\big(h(\underline{X})\big)$.Otherwise, the polynomial is said to be indecomposable.

In the remainder of this section, we consider only bivariate polynomials. In Section 3.1, we show how to reduce the study of multivariate polynomials to the study of bivariate polynomials.

We are looking for polynomials h such that $f = u \circ h$. Then $\deg f = \deg u \times \deg h$; thus $\deg h$ divides $\deg f$. Furthermore, if $f = u \circ h$ then we can suppose that $h(0,0) = 0$. Indeed, if $h(0,0) \neq 0$, we set $v = u\big(T + h(0,0)\big)$ and $H = h - h(0,0)$, then we get $f = v \circ H$ with $H(0,0) = 0$. This gives rise to the following definitions:

Definition 2. We denote by $E_{d_{min}}(f)$ the following set:

$$E_{d_{min}}(f) = \left\{ H(X,Y) \in \mathbb{K}[X,Y] \mid \deg H \leq \frac{\deg f}{d_{min}} \text{ and } H(0,0) = 0 \right\},$$

where d_{min} is the smallest prime dividing $\deg(f)$.

Definition 3. Let $f(X,Y) \in \mathbb{K}[X,Y]$ be a polynomial such that $\deg_X(f) > 0$ and $\deg_Y(f) > 0$. The $\mathbb{K}$-linear map

$$\begin{array}{rcl} Jac_f : E_{d_{min}}(f) & \longrightarrow & \mathbb{K}[X,Y] \\ H(X,Y) & \longmapsto & \partial_X f.\partial_Y H - \partial_Y f.\partial_X H \end{array}$$

is the restriction to $E_{d_{min}}(f)$ of the Jacobian derivation associated to f.

That is to say, $Jac_f(H) = \partial_X f.\partial_Y H - \partial_Y f.\partial_X H$ is the Jacobian of the polynomial map $(X,Y) \longmapsto \big(f(X,Y), H(X,Y)\big)$.

Most of our results rely on the following property of Jac_f.

Proposition 4. *Assume that $p = 0$ or $p > \dfrac{d^2}{d_{min}}$. Then*

$$Ker Jac_f \neq \{0\} \iff f = u \circ h,$$

where $h \in \mathbb{K}[X,Y]$ is an indecomposable polynomial, $u \in \mathbb{K}(T)$ and $\deg(u) \geq 2$.

This proposition is classical. We can find a general statement for $n \geq 2$ variables in [13, Theorem 6]. However, this result is usually stated with a separability hypothesis. In this paper, we want to obtain results with a hypothesis on the characteristic p of $\mathbb{K}$, such as is found in theorems about absolute factorization. For this reason, we give the proof of Proposition 4 to motivate the hypothesis on p.
A part of the proof of this proposition is based on the following lemma. This lemma is usually stated under the hypothesis $p = 0$ (see, for example, [24, Lemma 1.1]. We prove it in a more general case using a result of Jouanolou's work (see [14, Corollaire 7.2.2, p. 232]).

Lemma 5. *Let $f, g \in \mathbb{K}[X,Y]$ with f a non-constant polynomial, and assume that $p = 0$ or $p > \deg(f)\deg(g)$. If $Jac_f(g) = 0$, then f and g are algebraically dependent over $\mathbb{K}$.*

Proof. This proof follows very closely the proof of [24].
Assume that f and g are algebraically independent over $\mathbb{K}$. Then by Corollaire 7.2.2 in [14, p. 232], for every non-constant $P \in \mathbb{K}[X,Y]$ there exists a nonzero polynomial $\Phi(T_1,T_2,T_3) \in \mathbb{K}[T_1,T_2,T_3]$ such that $\Phi(f,g,P) = 0$ in $\mathbb{K}[X,Y]$ and $0 < \deg_{T_3}\Phi \leq \deg(f)\deg(g)$.
We rewrite this equality in the following way:

$$\sum_{i=0}^{s} \Phi_i(f,g)P^i = 0$$

where $\Phi_s \neq 0$ in $\mathbb{K}[X,Y]$ and $s \leq \deg(f)\deg(g)$. Without loss of generality, we can assume that s is minimal. Then by using the Leibniz rule and the assumption "$\mathrm{Jac}_f(g) = 0$", we obtain the following:

$$0 = Jac_f(\Phi(f,g,P)) = \Big(\sum_{i=1}^{s} i\Phi_i(f,g)P^{i-1}\Big)Jac_f(P).$$

If $s > 1$ then $\sum_{i=1}^{s} i\Phi_i(T_1,T_2)T_3^{i-1} \neq 0$ in $\mathbb{K}[T_1,T_2,T_3]$ because $s < p$. Thus $Jac_f(P) = 0$ because of the minimality of s.
If $s = 1$ then $\Phi_1(f,g)Jac_f(P) = 0$ and $\Phi_1(f,g) \neq 0$. So in all cases, we have $\mathrm{Jac}_f(P) = 0$ for each $P \in \mathbb{K}[X,Y]$ not equal to zero.
By using this result with $P = X$ and with $P = Y$, we get $\partial_X f = \partial_Y f = 0$. This implies that $f(X,Y) \in \mathbb{K}[X^p, Y^p]$ (since f is non-constant), and in particular, $\deg(f) > p$; this contradicts the assumption "$p > \deg(f)\deg(g)$". □

Now we prove Proposition 4.

Proof. $\Longrightarrow$) Let $H \in KerJac_f$ with $H \neq 0$. By Lemma 5 (with $g = H$), f and H are algebraically dependent over $\mathbb{K}$. Then by Gordan's Theorem [23, §1.2, Theorems 3 and 4], there exists a polynomial $h \in \mathbb{K}[X,Y]$ such that $f, H \in \mathbb{K}(h)$. Thus we have $f = u \circ h$ with $u(T) \in \mathbb{K}(T)$. As $f(X,Y)$ is a polynomial, $u(T)$ is necessarily in $\mathbb{K}[T]$. Moreover, $\deg(u) \geq 2$ since $d/d_{min} \geq \deg(H) \geq \deg(h)$ and $d = \deg(f) = \deg(u).\deg(h)$. Furthermore, one may assume that h is indecomposable (by taking $\deg(u)$ maximal).
$\Longleftarrow$) We just have to apply Jac_f to the condition $f = u \circ h$, to show that $h \in KerJac_f$. □

Remark 1.
(1) The following example shows that the same result is not true without the hypothesis $p > d^2/d_{min}$. Let $f(X,Y) = X^{p+1}Y \in \mathbb{K}[X,Y]$ where p is the characteristic of $\mathbb{K}$. The polynomial f is indecomposable, since $\deg_Y(f) = 1$, but $KerJac_f \neq \{0\}$ since $H(X,Y) = XY \in KerJac_f$.
(2) Throughout this article, the characteristic p of $\mathbb{K}$ is assumed to be either 0 or sufficiently large ($p > d^2/d_{min}$). It is well known (see [1, Theorem 7]) that in characteristic zero, we have an equivalence between "decomposable over $\mathbb{K}$" and "decomposable over any extension of $\mathbb{K}$". This equivalence cannot hold for positive characteristic in general [1, section 8].
However, it is true under the hypothesis $\gcd(p, \deg(f)) = 1$ for univariate polynomials (see [6]). Thus, using Kronecker's substitution (see [1]) we obtain the equivalence for multivariate polynomials under the hypothesis $\gcd(p, \deg(f)) = 1$. Refer to [2, Section 4, Theorem 4.2] for a general statement and more details.
Thus under the hypothesis that $p = 0$ or sufficiently large ($p > d^2/d_{min}$), f is decomposable over $\mathbb{K}$ if and only if f is decomposable over an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. Thus by abuse of notation we will sometimes write that f is decomposable instead of f is decomposable over its coefficient field.

3. Analogues to Bertini's and Noether's Theorems

3.1. Reduction from n to 2 variables.

In this subsection, we show that we can reduce the study of multivariate polynomials to the study of bivariate polynomials.

Proposition 6. *Let $d \geq 2$ be an integer and let*
$$f = \sum_{|\underline{e}| \leq d} c_{e_1,\dots,e_n} X_1^{e_1} \dots X_n^{e_n} \in \mathbb{K}[\underline{X}],$$
with $|\underline{e}| = e_1 + \dots + e_n$.
Let
$$\mathbb{L} := \mathbb{K}(\underline{U}, \underline{V}, \underline{W}) = \mathbb{K}(U_1, \dots, U_n, V_1, \dots, V_n, W_1, \dots, W_n),$$
where $U_1, \dots, U_n, V_1, \dots, V_n, W_1, \dots, W_n$ are algebraically independent variables. The bivariate polynomial
$$\tilde{f}(X,Y) = f(U_1X + V_1Y + W_1, \dots, U_nX + V_nY + W_n) \in \mathbb{L}[X,Y]$$
is indecomposable over $\overline{\mathbb{L}}$ if and only if f is indecomposable over $\overline{\mathbb{K}}$.

The proof of this proposition is closely related to the following classical result.

Lemma 7. *Let $f \in \mathbb{K}[\underline{X}]$ be a non-constant polynomial. We have:*
f is indecomposable over $\overline{\mathbb{K}}$ $\iff$ $f(\underline{X}) - T$ is irreducible in $\overline{\mathbb{K}(T)}[\underline{X}]$,
where T is a variable.

This lemma is an application of the well-known result of Bertini-Krull (see [23, Theorem 37, p. 217 and Corollary 1 p. 220]).

Now we prove Proposition 6.

Proof. By Lemma 7, $\tilde{f}(X,Y)$ is indecomposable over $\overline{\mathbb{L}}$ if and only if $\tilde{f}(X,Y) - T$ is irreducible in $\overline{\mathbb{L}(T)}[X,Y]$. By Lemma 7 in [15], this condition holds if and only if $f(\underline{X}) - T$ is irreducible in $\overline{\mathbb{K}(T)}[\underline{X}]$, or equivalently, if and only if $f(\underline{X})$ is indecomposable over $\overline{\mathbb{K}}$ (again by Lemma 7). □

Now we prove, with the help of an effective form of Bertini's Theorem for absolute factorization, the following effective result on reduction from n to 2 variables.

Theorem 8. *Let S be a finite subset of $\mathbb{K}$ and let $f \in \mathbb{K}[\underline{X}]$ be an indecomposable polynomial of total degree d. Suppose that $p = 0$ or $p > d(d-1)$. Then for a uniform random choice of u_i's, v_i's and w_i's in S, with probability at least $1 - (3d(d-1)+1)/|S|$, the polynomial*

$$\overline{f}(X,Y) = f(u_1X + v_1Y + w_1, \dots, u_nX + v_nY + w_n) \in \mathbb{K}[X,Y]$$

is indecomposable.

Proof. We want to show that the probability

$$\mathcal{P}\Big(\{\overline{f} \text{ is indecomposable } \mid f \text{ is indecomposable and } \underline{u}, \underline{v}, \underline{w} \in S\}\Big)$$

is at least equal to $1 - (3d(d-1)+1)/|S|$.

By Lemma 7, $f - T$ is irreducible over $\overline{\mathbb{K}(T)}[\underline{X}]$. Then, by Corollary 8 in [17], $\overline{f} - T$ is irreducible over $\overline{\mathbb{K}(T)}[X,Y]$ with probability at least $1 - (3d(d-1)+1)/|S|$. Remark that we can use Corollary 8 in [17] because $p = 0$ or $p > d(d-1)$.

By Lemma 7 applied to $\overline{f} - T$, we obtain the desired bound. □

3.2. **The set of decomposable polynomials.** In this section, we show that the set of decomposable polynomials is included in an algebraic variety. The inclusion is not trivial, that is, the algebraic variety is not of the form $\mathbb{K}^N$. The strategy is as follows: we use Proposition 6 to restrict our problem to the bivariate case, and then we use Proposition 4.

Theorem 9. *Let $d \geq 2$ and $n \geq 2$ be integers, and let $f = \sum_{|\underline{e}| \leq d} c_{\underline{e}} X_1^{e_1} \dots X_n^{e_n}$ be a non-constant polynomial with coefficients in $\mathbb{K}$. Assume that $p = 0$ or $p > d^2/d_{min}$. Then there exists a finite set of polynomials*

$$\Phi_1, \dots, \Phi_N \in \mathbb{Z}[C_{\underline{e}}] := \mathbb{E},$$

where the $C_{\underline{e}}$ are variables, $|\underline{e}| \leq d$, and N be an integer ≥ 2, with the following property:

$$\Phi_t(c_{\underline{e}}) = 0 \textit{ for all } t = 1, \dots, N \iff f \textit{ is decomposable or } \deg(f) < d.$$

Furthermore,

$$\deg(\Phi_t) \leq \frac{1}{2}\Big(\frac{d}{d_{min}} + 1\Big)\Big(\frac{d}{d_{min}} + 2\Big) + 1 =: \mathcal{B}$$

for all $t = 1, \dots, N$.

Remark 2.
(1) We can prove a version Theorem 9 without any hypothesis on the characteristic, but in this case the bound $\mathcal{B}$ is larger. Indeed, let Ψ_t be the Noether irreducibility forms associated to the polynomials $F = \sum F_{\underline{e}} X_1^{e_1} \dots X_n^{e_n} \in \mathbb{L}[\underline{X}]$ of degree d, where $\mathbb{L}$ is a field. By definition, the family $\{\Psi_t\}$ satisfies the following condition:

$$\forall t, \Psi_t(F_{\underline{e}}) = 0 \iff F(\underline{X}) \text{ is reducible over } \overline{\mathbb{L}} \text{ or } \deg(F) < d.$$

Now, we consider $f = \sum_{|\underline{e}| \leq d} c_{\underline{e}} X_1^{e_1} \dots X_n^{e_n}$, and we apply Noether's forms to $F = f - T \in \mathbb{K}[T][\underline{X}]$ and $\mathbb{L} = \mathbb{K}(T)$. Then $\Psi_t(F_{\underline{e}}) = \sum_{i \leq D} a_{t,i}(c_{\underline{e}}) T^i \in \mathbb{K}[T]$, with $D = \deg(\Psi_t)$, $a_{t,i} \in \mathbb{Z}[C_{\underline{e}}]$ where $C_{\underline{e}}$ are variables and $\deg(a_{t,i}) \leq D$. In this case, we have

$$\begin{aligned} \forall t, \forall i,\ a_{t,i}(c_{\underline{e}}) = 0 &\iff \forall t, \Psi_t(F_{\underline{e}}) = 0 \\ &\iff f - T \text{ is reducible over } \overline{\mathbb{K}(T)} \text{ or } \deg(f) < d \\ &\iff f \text{ is decomposable or } \deg(f) < d. \end{aligned}$$

Thus, the polynomials $a_{t,i}$ satisfy the same property as Φ_t in Theorem 9. Furthermore, $\deg(a_{t,i}) \leq \deg(\Psi_t)$. Unfortunately, as far as we know, the best bound for the degree of Noether's irreducibility forms in all characteristics is $\deg(\Psi_t) \leq 12d^6$ (see [15, Theorem 7]). This is the reason why we use another strategy for our proof to obtain a good bound for $\deg(\Phi_t)$.
(2) Theorem 9 is similar to the classical Noether's theorem on absolute factorization. Our bound is sharper than the one used for the absolute factorization. For example, if we have a polynomial of degree $d = 10$ then the degree of our forms is 22. But when we study the absolute factorization, the degree of Noether's absolute irreducibility forms are equal to $d^2 - 1 = 99$, see [21], [23, chapter 3]. As far as we know, there do not exist optimal results on the degree of Noether's absolute irreducibility forms. We also do not know if the bound given in Theorem 9 is optimal.

Now we prove Theorem 9.

Proof. We set the following notations:

- $F(\underline{X}) = \sum_{|\underline{e}| \leq d} C_{\underline{e}} X_1^{e_1} \dots X_n^{e_n}$, where $C_{\underline{e}}$ are variables, $F(\underline{X}) \in \mathbb{E}[\underline{X}]$,
- $\mathbb{L}' := \mathbb{E}(\underline{U}, \underline{V}, \underline{W})$,
- $\tilde{F}(X,Y) = F(U_1X + V_1Y + W_1, \dots, U_nX + V_nY + W_n) \in \mathbb{L}'[X,Y]$,
- $\{\Delta_s\}$ is the set of all maximal minors of the matrix $Jac_{\tilde{F}}$,
- $S := \{\tau \in \mathbb{E} \mid \tau \text{ is a coefficient of a term in } \underline{U}, \underline{V}, \underline{W} \text{ of some } \Delta_s\}$.

If we rewrite the proof of Theorem 3 in [16] with the matrix $Jac_{\tilde{F}}$ instead of Ruppert's matrix, then by Proposition 6 and Proposition 4, the set of indecomposability forms is

$$\{\Phi_t = C_{\underline{e}} \tau \in \mathbb{E} \mid |\underline{e}| = d,\ \tau \in S\}.$$

Thus, in order to bound $\deg \Phi_t$, we just have to bound $\deg \tau$. As $\deg \tau$ is bounded by the number of columns of $Jac_{\tilde{F}}$ the desired result follows. □

Now we are going to give a probabilistic corollary to Theorem 9.

Corollary 10. *Let $\mathbb{K}$ be a field of characteristic zero or $p > d^2/d_{min}$. Let $f(X_1, \dots, X_n) = \sum_{|\underline{e}| \leq d} c_{\underline{e}} X_1^{e_1} \dots X_n^{e_n} \in \mathbb{K}[\underline{X}]$, and S be a finite subset of $\mathbb{K}$.*

For a uniform random choice of $c_{\underline{e}}$ in S, the probability

$$\mathcal{P}\Big(\{f \text{ is indecomposable and } \deg f = d \mid c_{\underline{e}} \in S\}\Big)$$

is at least equal to $1 - \mathcal{B}/|S|$.

Proof. By Theorem 9, if f is decomposable or $\deg(f) < d$, then for all $t \in \{1, \dots, N\}$ we have $\Phi_t(c_{\underline{e}}) = 0$. Moreover, $\cap_{t=1}^{N}\{\Phi_t(c_{\underline{e}}) = 0\}$ is a subset of $\{\Phi_1(c_{\underline{e}}) = 0\}$. Thus the corollary follows from Theorem 9 and Zippel-Schwartz's lemma (see for example [25, Proposition 5], or [10, Lemma 6.44 p.174]). $\square$

3.3. **Indecomposable polynomials and specialization.** We study the specialization of an indecomposable polynomial with coefficients in $\mathbb{K}[T_1, \dots, T_m]$ where $T_1, \dots, T_m$ are new independent variables.

Theorem 11. *Assume that $p = 0$ or $p > d^2/d_{min}$. Let S be a finite subset of $\mathbb{K}$ and let*

$$f(T_1, \dots, T_m, \underline{X}) = \sum_{|\underline{e}| \leq d} a_{\underline{e}}(T_1, \dots, T_m)\underline{X}^{\underline{e}} \in \mathbb{K}[T_1, \dots, T_m][\underline{X}]$$

be an indecomposable polynomial over $\mathbb{K}(T_1, \dots, T_m)$ of total degree d. Suppose that $0 < \max(\deg(a_{\underline{e}})) \leq \mathfrak{D}$ and denote by $f_{\underline{\tau}}(\underline{X})$ the polynomial $f(\tau_1, \dots, \tau_m, \underline{X})$, where $\tau_1, \dots, \tau_m \in \mathbb{K}$. For a uniform random choice of τ_i's in S, with probability at least $1-\mathfrak{D}.\mathcal{B}/|S|$, the polynomial $f_{\underline{\tau}}(\underline{X})$ is indecomposable over $\mathbb{K}$ and $\deg(f) = \deg(f_{\underline{\tau}})$.

Proof. Since f is indecomposable over $\mathbb{K}(T_1, \dots, T_m)$, by Theorem 9, there exists $t \in \{1, \dots, N\}$ such that $\Phi_t\big(a_{\underline{e}}(\underline{T})\big) \neq 0$ in $\mathbb{K}[T_1, \dots, T_m]$, where $\deg \Phi_t\big(a_{\underline{e}}(\underline{T})\big) \leq \mathfrak{D}.\mathcal{B}$. Bad cases appear when we have $\Phi_t\big(a_{\underline{e}}(\underline{\tau})\big) = 0$ for all $t \in \{1, \dots, N\}$. Thus we get the desired estimate using Zippel-Schwartz's lemma as in Corollary 10. $\square$

Remark 3. We cannot obtain the same result if we use a substitution of the form $X_i = x_i$, for $i = 3, \dots, n$. For example, the polynomial $f(X_1, X_2, X_3) = X_1^6 X_2^{10} X_3^{15}$ is indecomposable. Indeed, if we write $f = u(h)$ then $\deg(u)$ divides $gcd(6, 10, 15) = 1$. But for all $x \in \mathbb{K}$, $f(x, X_2, X_3)$, $f(X_1, x, X_3)$, $f(X_1, X_2, x)$ are decomposable.

4. Analogues to Newton polygons and Ostrowski's theorem

4.1. **Decomposable polynomials and their Newton polygons.**

Definition 12. The support of $f(\underline{X})$ is the set S_f of integer points $(i_1, \dots, i_n)$ such that the monomial $X_1^{i_1} \cdots X_n^{i_n}$ appears in f with a non-zero coefficient.
We denote by $N(f)$ the convex hull (in the real space $\mathbb{R}^n$) of $S_f \cup \{(0, \dots, 0)\}$. This set $N(f)$ is called the Newton polygon of f.

Remark 4:
As f is decomposable if and only if $f + \lambda$ is decomposable, we have to add the origin to S_f when we compute the convex hull. Note that because $\{(0, \dots, 0)\}$ is added to S_f in our definition, we have $N(f) = N(f + \lambda)$ for all $\lambda \in \mathbb{K}$.

The next result is a necessary condition on the vertices of $N(f)$ for decomposable polynomials.

Proposition 13. *Let $f, h \in \mathbb{K}[\underline{X}]$, and $u \in \mathbb{K}[T]$ such that $f = u \circ h$. If $(i_1, \dots, i_n)$ is a vertex of $N(f)$ then we can write $(i_1, \dots, i_n) = (r.j_1, \dots, r.j_n)$, where $r = \deg(u)$ and $(j_1, \dots, j_n)$ is a vertex of $N(h)$.*

Proof. Note that we can restrict our study to the case $f(0, \dots, 0) \neq 0$. Indeed, as previously seen, f is decomposable if and only if $f + \lambda$ is decomposable for any $\lambda \in \mathbb{K}$. Moreover, $f = u \circ h$ implies $f = \prod_{k=1}^{r}(h - u_k)$, where $u_k \neq 0$ are the roots of u in $\overline{\mathbb{K}}$ and h is such that $h(0, \dots, 0) = 0$.
Recall that $f = f_1.f_2$ implies $N(f) = N(f_1) + N(f_2)$; see, for example, [8, Lemma 5], where the sum is the Minkowski sum of convex sets. Thus, we have $N(f) = \sum_{k=1}^{r} N(h - u_k)$. As the constant term of $h - u_k$ is not zero, all $h - u_k$ have the same support. This gives $N(f) = rN(h - u_1)$. □

4.2. **Indecomposability and reduction modulo p.** In the absolute factorization case, Ostrowski's Theorem states that "an absolutely irreducible integral polynomial remains absolutely irreducible modulo all sufficiently large prime numbers". For example, in [8, Theorem 1] the authors give (for $n = 2$) a sharp and effective bound for Ostrowski's theorem, namely $p > \Big(\sqrt{m^2 + n^2}.\|f\|_2\Big)^{2T-3}$, where T is the number of integral points in the Newton polygon of f, $m = \deg_X f$, $n = \deg_Y f$ and $\|f\|_2$ is the Euclidean norm of f. In this section, we use the same strategy with the Jacobian matrix. We show that if p is a large enough prime and f is indecomposable then $f \mod p$ is indecomposable. In the indecomposability case, the exponent $2T - 3$ of the previous bound becomes T.

Definition 14. Let $f \in \mathbb{K}[\underline{X}]$, $D = \gcd(i_1^{(1)}, \dots, i_n^{(1)}, \dots, i_1^{(k)}, \dots, i_n^{(k)})$ where $(i_1^{(\alpha)}, \dots, i_n^{(\alpha)})$ are the coordinates of the vertices of $N(f)$. Let D_{min} be the smallest prime dividing D.

Let $N(f)_{D_{min}}$ be the polygon with vertices $\Big(\dfrac{i_1^{(\alpha)}}{D_{min}}, \dots, \dfrac{i_n^{(\alpha)}}{D_{min}}\Big)$.
We denote by $\mathcal{E}$ the following set:
$\mathcal{E} = \{P(\underline{X}) \in \mathbb{K}[\underline{X}] \mid S_P \subset N(f)_{D_{min}} \text{ and } P(0, \dots, 0) = 0\}$.

Theorem 15. *Let $f = \sum_{i,j} c_{i,j} X^i Y^j \in \mathbb{Z}[X, Y]$ be an indecomposable polynomial of degree d.
Let $H(f)$ be the height of f, that is, $H(f) = \max_{i,j} |c_{i,j}|$.
If $D = 1$, then for every prime such that $p > H(f)$, $f \mod p$ is indecomposable.
If $D \neq 1$, then $f \mod p$ is indecomposable for every prime p such that $p > \max\Big[\dfrac{d^2}{d_{min}}, \Big(\dfrac{d^2}{D_{min}}\|f\|_2\Big)^{T'}\Big]$, where T' is the number of integral points in $N(f)_{D_{min}}$.*

Proof. If $D = 1$, then the result is a consequence of Proposition 13:
indeed, if $p > H(f)$ then $N(f) = N(f \mod p)$. Thus, the coordinates of the vertices of $N(f \mod p)$ are relatively prime, and by Proposition 13 it follows that $f \mod p$ is indecomposable.

If $D \neq 1$, we follow the strategy given in [8].
By Proposition 13, we can restrict Jac_f to $\mathcal{E}$ and as $p > d^2/d_{min}$ Proposition 4 implies:

$$(\star)\ \dim_{\mathbb{K}} KerJac_{f/\mathcal{E}} = 0 \iff f \text{ is indecomposable.}$$

Now, we just have to show that the dimension of the kernel remains equal to zero after the reduction of $f \mod p$.
Since f is indecomposable, $Jac_{f/\mathcal{E}}$ has rank T'. Then there exists a submatrix M of $Jac_{f/\mathcal{E}}$ such that rank $M = T'$. Now we are going to estimate $\det M$ using Hadamard's inequality.
Each column of $Jac_{f/\mathcal{E}}$ corresponds to a polynomial of the following form: $Jac_{f/\mathcal{E}}(X^aY^b) = (\partial_X f)bX^aY^{b-1} - (\partial_Y f)aX^{a-1}Y^b$, where $(a,b) \in N(f)_{D_{min}}$. Thus a and b are less than d/D_{min}.
Moreover, $Jac_{f/\mathcal{E}}(X^aY^b) = \sum_{i,j}(ib-aj)c_{i,j}X^{a+i-1}Y^{b+j-1}$, where i and j are smaller than d. Thus each column has norm less than $\dfrac{d^2}{D_{min}}\|f\|_2$. Hence, Hadamard's inequality,

$$|\det M| \leq \Big(\frac{d^2}{D_{min}}\|f\|_2\Big)^{T'}.$$

Thus if $p > \Big(\dfrac{d^2}{D_{min}}\|f\|_2\Big)^{T'}$, then $Jac_{f/\mathcal{E}} \mod p$ has full rank. Here $Jac_{f/\mathcal{E}} \mod p$ means that all coefficients of $Jac_{f/\mathcal{E}}$ are reduced modulo p. This matrix is $Jac_{f \mod p/\mathcal{E}}$.
Thus, if $p > \max\Big[\dfrac{d^2}{d_{min}}, \Big(\dfrac{d^2}{D_{min}}\|f\|_2\Big)^{T'}\Big]$, then $Jac_{f \mod p/\mathcal{E}}$ has full rank, and we can apply the property $(\star)$. Thus $f \mod p$ is indecomposable. $\square$

5. An indecomposability test

Several efficient algorithms for decomposing a polynomial are given in the literature (see, e.g., [5, 9, 12]). The algorithm given in [9] is nearly optimal. However, it is sometimes useful to have an easy test for hand computations. For example, if we want to check that

$$f(X,Y) = X^d + X^{d/2}Y^{d/2-1} + \sum_{i=1}^{d/2-1}\sum_{j=1}^{d/2-2}\big(2^{2^{d+i+j}}-1\big)X^iY^j + 3, \text{ with } d = 2k,\ k \geq 2,$$

is indecomposable, then the computation requires at least $O(2^d)$ bit operations. Indeed, the length of the coefficients is $O(2^d)$. With the following test, we can conclude that this polynomial is indecomposable, and avoid a computation with an exponential (relatively to d) bit complexity.

Our test is a direct corollary of Proposition 13, and this idea has already been used for Theorem 15. A similar test for the absolute factorization has already been studied in [3, Chapitre 5].

Corollary 16. *Let* $(i_1^{(1)}, \dots, i_n^{(1)}, \dots, i_1^{(k)}, \dots, i_n^{(k)})$ *be the vertices of* $N(f)$.
If $\gcd(i_1^{(1)}, \dots, i_n^{(1)}, \dots, i_1^{(k)}, \dots, i_n^{(k)}) = 1$ *then* f *is indecomposable.*

Remark 5:
(1) If $(d/2, d/2-1)$ is a vertex of $N(f)$ in the previous example and $d/2$, $d/2-1$ are coprime, then f is indecomposable.
(2) The "speed" of our test does not depend of $\mathbb{K}$, but only on $N(f)$. That is, our test performs the same computations with f as with

$$g(X,Y) = X^d + X^{d/2}Y^{d/2-1} + \sum_{i=1}^{d/2-1}\sum_{j=1}^{d/2-2} P_{i,j}(T)X^iY^j + 3 \in \mathbb{Q}(T)[X,Y],$$

where $P_{i,j}(T) \in \mathbb{Q}(T)$. (Thus g is indecomposable.)
(3) If we do not add the origin to the support, then Corollary 16 is false: consider $h(X,Y) = X^4Y^2 + X^5Y^5 + X^2Y$ and $f(X,Y) = h^2 - h$. Then f is decomposable but $(2,1)$, $(8,4)$, $(10,10)$, $(5,5)$ are the vertices of S_f and $\gcd(2,1,8,4,10,5) = 1$.

Thus, we have produced a simple test for the indecomposability of a polynomial.

If the coordinates of the vertices of $N(f)$ are $(0,\dots,0)$, $(d,0,\dots,0)$, $(0,\dots,d)$ then our test returns "I don't know". This situation appears when all the coefficients of f in the dense representation are non-zero. However, if a lot of coefficients of f in the dense representation are equal to zero, then using Corollary 16 we can often quickly detect if f is indecomposable. The following table gathers some statistical evidence about this claim. This test has been implemented in MAGMA [18], and is freely available at http ://www.math.univ-toulouse.fr/∼cheze/.

d	$Sparse$	$Success$	T_{avg}	T_{max}	T_{min}
10	0%	0	0.00015	0.011	0
10	50%	711	0.00007	0.011	0
10	66%	837	0.00009	0.011	0
10	90%	914	0.0009	0.011	0
100	66%	836	0.013	0.021	0
200	66%	848	0.1821	0.23	0.13

FIGURE 1. Some results of our test.

We randomly constructed 1000 polynomials of total degree d with two variables. $Sparse$ denotes the ratio of null coefficients in the dense representation for the total degree d. For example "$Sparse = 66\%$ " means that 66% of the coefficients are equal to zero in the dense representation for the total degree d. The coefficients of f belong to $[-10^{12}; 10^{12}]$. $Success$ is the number of indecomposable polynomials detected with our test. T_{avg} (resp. T_{max}, T_{min}) is the average (resp. maximum, minimum) timing in seconds to perform one test.
This table shows that our test is well suited for sparse polynomials.
As the number n of variables, increases the probability of success increases with n. Indeed, when a polynomial has n variables, each vertex of its Newton polygon has n coordinates. Thus the number of coordinates increases, and thus the chance of obtaining a gcd equal to 1. Our implementation relies on the Magma function: *NewtonPolygon*. Unfortunately, this function only works for bivariate polynomials. For this reason, our table only shows numerical evidence for bivariate polynomials.

6. ACKNOWLEDGMENTS

The authors thank Arnaud Bodin, Pierre Dèbes, Joachim von zur Gathen, Grégoire Lecerf and Laurent Busé for their valuable comments. The second author was supported by the "Abdus Salam" center, ICTP, Trieste (Italy); for this he wishes to thank all staff of this center.

REFERENCES

[1] M. Ayad, *Sur les polynômes $f(X,Y)$ tels que $K[f]$ est intégralement fermé dans $K[X,Y]$,* Acta Arith. 105 (2002), 9–28.

[2] A. Bodin, P. Dèbes, S. Najib, *Indecomposable polynomials and their spectrum,* Acta Arith.(to appear).

[3] G. Chèze, *Des méthodes symboliques-numériques et exactes pour la factorisation absolue des polynômes en deux variables,* Thèse de Doctorat, Univ. Nice-Sophia Antipolis (2004).

[4] G. Chèze, G. Lecerf, *Lifting and Recombination Techniques for Absolute Factorization*, Journal of Complexity (2007), 23 (3), 380–420.

[5] M. Dickerson, *Functional Decomposition of Polynomials*, Tech. Rep. 89-1023, Department of Computer Science, Cornell University, Ithaca NY, (1989).

[6] M. Fried, R.E.Mac Rae, *On the invariance of chains of fields*, Illinois J. Math. 13 (1969), 165–171.

[7] S. Gao, *Factoring multivariate polynomials via partial differential equations,* Math. Comp. 72 (2003), 801–822.

[8] S. Gao, V. Rodrigues, *Irreducibility of polynomials modulo p via Newton polytopes,* J. Number Theory, 101 (2003), 32–47.

[9] J. von zur Gathen, *Functional decomposition of polynomials: the tame case,* J. Symbolic Comput. 9(3) (1990), 281–299.

[10] J. von zur Gathen and J. Gerhard, *Modern computer algebra.* Cambridge University Press, second edition, 2003.

[11] J. von zur Gathen, J. Gutierrez, R. Rubio, *Multivariate polynomial decomposition*, Appl. Algebra Engrg. Comm. Comput. 14 (2003), 11–31.

[12] J. Gutierrez, R. Rubio, D. Sevilla, *Unirational fields of transcendence degree one and functional decomposition*, ISSAC '01: Proceedings of the 2001 international symposium on Symbolic and algebraic computation, (2001), 167–174, London, Ontario, Canada.

[13] J. Gutierrez, D. Sevilla, *Computation of unirational fields*, J. Symbolic Comput. 41 (2006), 1222–1244.

[14] J.-P. Jouanolou, *Le formalisme du résultant*, Adv. Math. 90 (1991), 117–263.

[15] E. Kaltofen, *Effective Noether irreducibility forms and applications*, J. Computer and System Sciences 50 (1995), 274–295.

[16] E. Kaltofen, J. May, *On approximate irreducibility of polynomials in several variables,* Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 161–168 (electronic).

[17] G. Lecerf, *Improved dense multivariate polynomial factorization algorithms,* J. Symbolic Comput. 42 (2007), 477–494.

[18] The Magma computational algebra system for algebra, number theory and geometry. http://magma.maths.usyd.edu.au/magma/. Computational Algebra Group, School of Mathematics and Statistics, The University of Sydney, NSW 2006 Australia.

[19] S. Najib, *Factorisation des polynômes* $P(X_1,\dots,X_n)-\lambda$ *et théorème de Stein*, Thèse de Doctorat. Univ. Lille 1 (2005).

[20] W. M. Ruppert, *Reducibility of polynomials* $f(x,y)$ *modulo* p, J. Number Theory, 77 (1999) 62–70.

[21] W. M. Ruppert, *Reduzibilität ebener Kurven*, J. Reine Angew. Math. 369 (1986), 167–191.

[22] Peter Scheiblechner, *On the complexity of counting irreducible components and computing betti numbers of algebraic variety.* PhD thesis, University of Paderborn, 2007.

[23] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, 77. Cambridge University, 2000.

[24] Y. Stein, *The total reducibility order of a polynomial in two variables*, Isr. J. Math. 68 (1989), 109–122.

[25] R. Zippel, *Zero testing of algebraic functions*, Information Processing Letters 61 (1997), 63–67.

Institut de Mathématiques de Toulouse, Université Paul Sabatier Toulouse 3, MIP Bât 1R3,, 31 062 TOULOUSE cedex 9, FRANCE

E-mail address: guillaume.cheze@math.univ-toulouse.fr

ICTP, The Abdus Salam International Centre for Theoretical Physics. Strada Costiera, 11, 34014 Trieste, ITALY

E-mail address: snajib@ictp.it, salah.najib@math.univ-lille1.fr