Available at: http://publications.ictp.it IC/2007/128

United Nations Educational, Scientific and Cultural Organization
and
International Atomic Energy Agency
THE ABDUS SALAM INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

INDECOMPOSABILITY OF POLYNOMIALS VIA JACOBIAN MATRIX

Guillaume Chèze[1]
Institut de Mathématiques de Toulouse, Université Paul Sabatier Toulouse 3, MIP Bât 1R3, 31 062 Toulouse Cedex 9, France

and

Salah Najib[2]
The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

Abstract

Uni-multivariate decomposition of polynomials is a special case of absolute factorization. Recently, thanks to the Ruppert's matrix some effective results about absolute factorization have been improved. Here we show that with a jacobian matrix we can get sharper bounds for the special case of uni-multivariate decomposition.

MIRAMARE – TRIESTE
December 2007

[1]guillaume.cheze@math.ups-tlse.fr
[2]snajib@ictp.it; salah.najib@math.univ-lille1.fr

1. Introduction

In this paper we study the decomposition of multivariate polynomials. Let $\mathbb{K}$ be a field. We say that a polynomial $f(X_1,\ldots,X_n) \in \mathbb{K}[X_1,\ldots,X_n]$ is decomposable over $\mathbb{K}$ if and only if there exist polynomials $u(T) \in \mathbb{K}[T]$ and $h(X_1,\ldots,X_n) \in \mathbb{K}[X_1,\ldots,X_n]$ such that $f(X_1,\ldots,X_n) = u\big(h(X_1,\ldots,X_n)\big)$ and $\deg(u) \geq 2$. This decomposition is called *uni-multivariate decomposition of f*. If such a decomposition does not exist then we say that f is indecomposable.

In this article we suppose that the characteristic p of $\mathbb{K}$ is 0 or large enough (this implies $p > \deg f$, see Theorem 1 for a more precise statement). It is well known (see [2] Theorem 7) that in the characteristic zero case, we have equivalence between "decomposable over $\mathbb{K}$" and "decomposable over any extension of $\mathbb{K}$". But this equivalence cannot hold for positive characteristic in general [1, 2]. For the one variable case, this equivalence is true under the hypothesis $\gcd(p,\deg(f)) = 1$ [9]. Thus, one can use this fact and Kronecker's substitution (see [2]) for showing the equivalence for multivariate polynomials under our hypothesis "p large enough" (see [3] for more details). Thus in this paper f is decomposable over $\mathbb{K}$ is equivalent to f is decomposable over $\overline{\mathbb{K}}$, where $\overline{\mathbb{K}}$ is an algebraic closure of $\mathbb{K}$. That's why we will sometimes write f is decomposable instead of f is decomposable over its coefficients field.

Uni-multivariate decomposition is a special case of absolute factorization (that is to say the factorization in $\overline{\mathbb{K}}[X,Y]$). 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 [23, 10, 16]) study the behaviour of the absolute factorization after some perturbations: reduction modulo p, reduction from n to 2 variables. The key point of all these problems is that we can reduce them to linear algebra. For the absolute factorization the matrix used comes from the computation of the first de Rham's cohomology group of the complementary of a plane curve [23, 6]. We called this matrix the Ruppert's matrix (see [23], [24] chapter 3). In this paper we show that we can also use a matrix Jac_f in order to study the uni-multivariate decomposition of f. This matrix comes from the study of a jacobian equation. Thanks to this matrix we get bounds dedicated to the uni-multivariate decomposition problem.

In the first section we give some motivations for the study of uni-multivariate decomposition. In the second section we recall some results about uni-multivariate decomposition and the jacobian matrix. These results are well known in characteristic zero. Here we extend these results to the positive characteristic. Then in order to have a self contained paper we show that the "usual proof" works in a more general context. These results state that the uni-multivariate decomposition problem can be solved using only linear algebra.

In Section 3 we give some analogous of well known irreducibilty theorems in our indecomposability context. We show that the set of decomposable polynomials is an algebraic variety, and we give bound on the degree of the equations of this variety. Next we use this result in order

to show how we can restrict the study of a multivariate polynomial to the study of a bivariate polynomial. (This kind of results for the absolute factorization are called Noether's and Bertini's theorem, see [10, 15, 16, 17, 23], and [4] chapitre 1.)

In Section 4, we study the reduction modulo p of an indecomposable polynomial with integer coefficients. In the absolute factorization context we have the Ostrowski's theorem: In 1919 Ostrowski established that an absolutely irreducible integral polynomial remains absolutely irreducible modulo all sufficiently large prime numbers. In [11] the authors give a sharp and effective bound for the Ostrowski's problem. The bound is the following $p > \left(\sqrt{m^2+n^2}.\|f\|_2\right)^{2T-3}$ where T is the number of integral points in the Newton's polygon of f, $m = \deg_X f$, $\deg_Y f = n$ and $\|f\|_2$ is the Euclidean norm of f. The authors applied Hadamard's inequality to the Ruppert's matrix and use some properties of the Newton's polygon. Here we use the same strategy with our jacobian matrix and we show that if p is large enough then f is indecomposable implies that $f \mod p$ is indecomposable. In the uni-multivariate decomposition case the exponent $2T-3$ of the previous bound becomes T.

At last in Section 5, we use a property of Newton's polygons to get an efficient symbolic indecomposability test. Some timings are given in order to show the efficiency of this test.

1.1. **Motivations of our work.** Uni-multivariate decomposition of polynomials has a theoretical meaning.

First, we have the following equivalence: f is indecomposable if and only if f is closed (that is to say: $\mathbb{K}[f]$ is integrally closed in $\mathbb{K}[X,Y]$, see [1], [2]).

Furthermore, indecomposability is a necessary condition when we study the spectrum of a polynomial. The spectrum $Spect(f)$ of a polynomial f is the set of λ such that $f+\lambda$ is reducible in $\overline{\mathbb{K}}[X,Y]$. If f is indecomposable then $Spect(f)$ is finite (see [1], or [24] chapter 3, corollary 1 page 220 for the case $\mathbb{K} = \overline{\mathbb{K}}$). Thus the decomposition of polynomials is related to the study of the spectrum. Stein's theorem (see [26], [18], [8] and [20]) gives an optimal bound for the cardinal of $Spect(f)$. In our paper we follow Stein's method because it needs only linear algebra. We get thus a matrix which plays the same role as Ruppert's matrix for the absolute factorization.

Another motivation for the study of uni-multivariate decomposition is the link with intermediate fields between $\mathbb{K}(f)$ and $\mathbb{K}(X,Y)$. Indeed, we have the following equivalence (see [28]): The equivalence classes of uni-multivariate decompositions of a nonconstant polynomial $f \in \mathbb{K}[X,Y]$ corresponds bijectively to intermediate fields $\mathbb{F}$ with transcendence degree 1 over $\mathbb{K}$ and such that $\mathbb{K}(f) \subset \mathbb{F} \subset \mathbb{K}(X,Y)$. For a study of computations of intermediate fields we can read: [12], [13] and references therein.

For an algorithmic point of view about this problem we can read for example [27], [13], [7] and references therein, and for an approximate point of view [5].

1.2. **Notation.** For a field $\mathbb{F}$, we denote by $\overline{\mathbb{F}}$ one of these algebraic closures.

p is the characteristic of $\mathbb{K}$.

$\deg(f)$ is the total degree of f.
$f(\underline{X})$ means $f(X_1, \ldots, X_n)$ with $n \geq 2$.
$f(\underline{X}) = u(h(\underline{X}))$ is written $f = u \circ h$.
$\partial_{X_i} f$ denotes the partial derivative of f with respect to X_i.
$trdeg_{\mathbb{K}}\mathbb{F}$ denotes the transcendance degree of $\mathbb{F}$ over $\mathbb{K}$.

2. Jacobian derivation and uni-multivariate decomposition

2.1. **Algebraic dependence and the jacobian.** In this section we present our toolbox.

Definition 1. *Let $2 < i < n$, I a subset of $\{2, \ldots, n\}$, $\mathbb{K}(\underline{X}, \widehat{X}_{1,I})$ is the field $\mathbb{K}(X_{j,j\in\{2,\ldots,n\}\setminus I})$.*

Definition 2. *Let $f \in \mathbb{K}[\underline{X}]$. We denote by $D_{f,i}$ the following derivation on $\mathbb{K}(\underline{X}, \widehat{X}_{1,i})[X_1, X_i]$.*

$$\begin{aligned} D_{f,i} : \mathbb{K}(\underline{X}, \widehat{X}_{1,i})[X_1, X_i] &\longrightarrow \mathbb{K}(\underline{X}, \widehat{X}_{1,i})[X_1, X_i] \\ H(X_1, X_i) &\longmapsto \partial_{X_1} f . \partial_{X_i} H - \partial_{X_i} f . \partial_{X_1} H \end{aligned}$$

$D_{f,i}(H)$ is the jacobian of the polynomial map: $(X_1, X_i) \longmapsto (f, H)$.

Our work is based on the following lemmas. These lemmas are short generalizations of a part of Lemma 1.1 in [26]. These lemmas are usually stated with the hypothesis $p = 0$. Here we prove them in a more general case thanks to the following result. This result is the classical result from elimination theory.

Lemma 1. *Let $\mathbb{K}$ be a field and $n \geq 1$ be an integer.*
Assume given $n+1$ polynomials $P_1, \ldots, P_{n+1} \in \mathbb{K}[X_1, \ldots, X_n]$ and, for all $j \in \{1, \ldots, n+1\}$, there exists an integer $d_j \geq 1$ such that $\deg(P_j) \leq d_j$. Then there exists a nonzero polynomial $\Phi \in \mathbb{K}[T_1, \ldots, T_{n+1}]$, of the form

$$\Phi = \sum_{d_1\alpha_1 + \ldots + d_{n+1}\alpha_{n+1} \leq d_1 \ldots d_{n+1}} c_{\alpha_1,\ldots,\alpha_{n+1}} T_1^{\alpha_1} \ldots T_{n+1}^{\alpha_{n+1}} \quad (c_{\alpha_1,\ldots,\alpha_n} \in \mathbb{K}),$$

such that $\Phi(P_1, \ldots, P_{n+1}) = 0$ in $\mathbb{K}[X_1, \ldots, X_n]$.

Proof. See [14] corollaire 7.2.2, p. 232 for a proof of this lemma. □

Lemma 2. *Let $f, g \in \mathbb{K}[\underline{X}]$, f is non-constant, and $p = 0$ or $p > \deg(f)\deg(g)$. Then we have: If $D_{f,i}(g) = 0$ then f and g are algebraically dependent over $\mathbb{K}(\underline{X}, \widehat{X}_{1,i})$.*

Proof. Of course this proof follows very closely the proof of [26].
Assume that f and g are algebraically independent over $\mathbb{K}(\underline{X}, \widehat{X}_{1,i})$. Then by lemma 1, for every non-constant $P \in \mathbb{K}(\underline{X}, \widehat{X}_{1,i})[X_1, X_i]$ 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 $\mathbb{K}[X_1, X_i]$ and $0 < \deg_{T_3} \Phi \leq \deg(f)\deg(g)$.
We rewrite this equality in the following way:

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

where $\Phi_n \neq 0$ in $\mathbb{K}(\underline{X}, \widehat{X}_{1,i})[X_1, X_i]$ and $n \leq \deg(f)\deg(g)$. We can assume n to be the least possible for P. Then:

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

If $n > 1$ then $\sum_{i=1}^{n} i\Phi_i(T_1, T_2)T_3^{i-1} \neq 0$ in $\mathbb{K}[T_1, T_2, T_3]$ because $n < p$. Thus $[f, P] = 0$ because of the minimality of n.
If $n = 1$ then $\Phi_1(f, g)[f, P] = 0$ and $\Phi_1(f, g) \neq 0$. Thus $[f, P] = 0$ for each $P \in \mathbb{K}(\underline{X}, \widehat{X}_{1,i})[X_1, X_i]$. We use this result with $P = X_1$ and next with $P = X_i$. We get $\partial_{X_1} f = \partial_{X_i} f = 0$. This means $f(\underline{X}) \in \mathbb{K}(\underline{X}, \widehat{X}_{1,i})[X_1^p, X_i^p]$, thus $\deg f > p$ and we get a contradiction. □

Lemma 3. *We denote by $\mathfrak{S}_{n-1}$ the group of all permutations of the set $\{2, \ldots, n\}$.*
Let $2 \leq k \leq n$ and $f, g \in \mathbb{K}[\underline{X}]$ such that for all i $\deg_{X_i} f > 0$ and :

$$\forall \sigma \in \mathfrak{S}_{n-1},\ f \text{ and } g \text{ are algebraically dependent over } \mathbb{K}(\underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k)})$$

then

$$\forall \sigma \in \mathfrak{S}_{n-1},\ f \text{ and } g \text{ are algebraically dependent over } \mathbb{K}(\underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k),\sigma(k+1)})$$

Proof. As f and g are algebraically dependent over $\mathbb{K}(\underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k)})$ there exists a polynomial P such that $P(f, g, \underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k)}) = 0$.
If $d_1 = \deg_{X_{\sigma(k+1)}} P(0, 0, \underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k)}) = 0$ then f and g are algebraically dependent over $\mathbb{K}(\underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k)})$ and we get the desired result.
We also have f and g are algebraically dependent over $\mathbb{K}(\underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k-1),\sigma(k+1)})$. Then there exists a polynomial Q such that $Q(f, g, \underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k-1),\sigma(k+1)}) = 0$.
As before if $d_2 = \deg_{X_{\sigma(k)}} Q(0, 0, \underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k-1),\sigma(k+1)}) = 0$ then as before we get the desired result.
Now we suppose that $d_1 > 0$ and $d_2 > 0$ this means that $X_{\sigma(k+1)}$ and $X_{\sigma(k)}$ are algebraic over $\mathbb{K}(f, g, \underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k-1),\sigma(k),\sigma(k+1)})$.
This gives $trdeg_{\mathbb{K}}\mathbb{K}(f, g, \underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k+1)}) = trdeg_{\mathbb{K}}\mathbb{K}(f, g, \underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k-1)})$.
However $trdeg_{\mathbb{K}}\mathbb{K}(f, g, \underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k+1)}) \leq n - k + 1$ and
$trdeg_{\mathbb{K}}\mathbb{K}(f, g, \underline{X}, \widehat{X}_{1,\sigma(2),\ldots,\sigma(k-1)} \geq n - k + 2$ because $\deg_{X_i} f > 0$.
Thus we get a contradiction and this concludes the proof. □

The following lemma is a corollary of Luröth's theorem (see [12] for a constructive proof of this theorem, or see Gordan's theorem in [24] page 15).

Lemma 4. *Let $\mathbb{K}$ be a field. If non-constant polynomials $f, g \in \mathbb{K}[\underline{X}]$ are algebraically dependent over $\mathbb{K}$ then there exists an indecomposable polynomial $h \in \mathbb{K}[\underline{X}]$ such that $f, g \in \mathbb{K}[h]$.*

Proof. If f and g are algebraically dependent over $\mathbb{K}$ then the transcendance degree of $\mathbb{K}(f,g)$ over $\mathbb{K}$ is one. Then by Luröth's theorem we can write $\mathbb{K}[f,g]=\mathbb{K}[h]$, where h is a polynomial. If h is indecomposable we are done, and if $h=u\circ H$ with H indecomposable then $f,g\in\mathbb{K}[H]$. □

2.2. **Linear algebra and uni-multivariate decomposition.** We are looking for polynomials h such that $f=u\circ h$ then $\deg f=\deg u\times\deg h$. Thus $\deg h$ divides d, this leads to the following definition:

Definition 3. *We denote by $E_{d_{min}}$ the following set:*

$$E_{d_{min}}=\left\{H(\underline{X})\in\mathbb{K}[\underline{X}]\mid \deg H\leq\frac{d}{d_{min}}\ \textit{and}\ H(0,\ldots,0)=0\right\},$$

where d_{min} is the smallest prime dividing $\deg(f)=d$.
We denote by $D_{f,i/E_{d_{min}}}$ the map $D_{f,i}$ restricted to $E_{d_{min}}$.

Theorem 1. *We assume that $p=0$ or $p>\dfrac{d^2}{d_{min}}$.*
Let $f\in\mathbb{K}[\underline{X}]$ such that for all $i=1,\ldots,n$, $\deg_{X_i}f>0$.
We have

$$\bigcap_{i=2}^{n}KerD_{f,i/E_{d_{min}}}\neq\{0\}\iff f=u\circ h,$$

where h is an indecomposable polynomial and $\deg(u)\geq 2$.

Proof. $\Longrightarrow$) Let $H\in\bigcap_{i=2}^{n}KerD_{f,i/E_{d_{min}}}$ with $H\neq 0$. We apply lemma 2 and we get that f and H are algebraically dependent over $\mathbb{K}(\underline{X},\widehat{X}_{1,i})$ for all $i=2,\ldots,n$. Then we apply lemma 3 and we get that f and H are algebraically dependent over $\mathbb{K}$. Then lemma 4 implies $f,H\in\mathbb{K}[h]$ with h indecomposable. Thus we have $f=u\circ h$. Furthermore $\deg(u)\geq 2$ because $d/d_{min}\geq\deg H\geq\deg h$, and $d=\deg f=\deg u.\deg h$.
$\Longleftarrow$) We just have to derive $f=u\circ h$, and we show that $h\in KerD_{f,i/E_{d_{min}}}$. □

In the bivariate case we get:

Corollary 1. *We assume that $p=0$ or $p>\dfrac{d^2}{d_{min}}$. Let $f\in\mathbb{K}[X,Y]$ such that $\deg_X f>0$ and $\deg_Y f>0$. We consider the following $\mathbb{K}$-linear map:*

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

Then we have:

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

where h is an indecomposable polynomial and $\deg(u)\geq 2$.

Remarks:

(1) $\partial_X f.\partial_Y H-\partial_Y f.\partial_X$ is the jacobian of the polynomial map:
$(X,Y)\longmapsto\big(f(X,Y),g(X,Y)\big)$.

(2) $\bigcap_{i=2}^{n} KerD_{f,i} \neq \{0\}$ means that there exists a polynomial $H(\underline{X})$ such that the jacobian of the polynomial map $\underline{X} \longmapsto \big(f(\underline{X}), H(\underline{X})\big)$ is not zero.

(3) A natural question arises: Can we get the same result without the hypothesis: $p > d^2$? This example shows that it is not obvious. Let $f(X,Y) = X^{p+1}Y \in \mathbb{K}[X,Y]$ where p is the characteristic of $\mathbb{K}$. f is indecomposable because $\deg_Y f = 1$ and $KerJac_f \neq \{0\}$. Indeed $H(X,Y) = XY \in KerJac_f$.

(4) We have already remarked that uni-multivariate decomposition is a kind of absolute factorization. For the absolute factorization we can also study the problem with a kernel of a differential equation (see [22], [10]). In this case we solve: $f(\partial_Y g - \partial_X h) + h\partial_X f - g\partial_Y f = 0$, where g and h are unknowns.
There is a link with our equation. We just have to set $\partial_Y H = h$ and $\partial_X H = g$ and we get our jacobian formulation. Thus, our matrix is a special case of the Ruppert-Gao's matrix.

3. Bertini's and Noether's like theorems

Decomposable polynomials give an algebraic variety. Here we bound the equations of this variety. Then we show that we can reduce the study of multivariate polynomials to the study of bivariate polynomials.

Theorem 2. *Let*

$$f = \sum_{|\underline{e}| \leq d} c_{e_1,\ldots,e_n} X_1^{e_1} \ldots X_n^{e_n} \in \mathbb{K}[X_1, \ldots, X_n],$$

with $\mathbb{K}$ a field of characteristic is 0 or $p > d^2/d_{min}$ and $|\underline{e}| = e_1 + \cdots + e_n$.
Let

$$\mathbb{L} := \mathbb{K}(\underline{U}, \underline{V}, \underline{W}) := \mathbb{K}(U_1, \ldots, U_n, V_1, \ldots, V_n, W_1, \ldots, W_n),$$

where $U_1, \ldots, U_n, V_1, \ldots, V_n, W_1, \ldots, W_n$ are algebraically independent variables. The bivariate polynomial

$$\tilde{f}(X,Y) = f(U_1X + V_1Y + W_1, \ldots, U_nX + V_nY + W_n) \in \mathbb{L}[X,Y]$$

is indecomposable over $\mathbb{L}$ if and only if f is indecomposable over $\mathbb{K}$.

The proof of theorem 2 is closely related to two following classical lemmas:

Lemma 5. *We use the same notation and hypothesis as in Theorem 2. We have*
$\tilde{f}(X,Y)$ is irreducible in $\overline{\mathbb{L}}[X,Y] \iff f(\underline{X})$ is irreducible in $\overline{\mathbb{K}}[\underline{X}]$.

Proof. For a proof of this classical lemma see [15] lemma 7. □

Lemma 6. *Let $\mathbb{K}$ be a field and $f \in \mathbb{K}[\underline{X}]$ be a non-constant polynomial. We have the following equivalence:*
f is decomposable over $\mathbb{K} \iff f(\underline{X}) - T$ is reducible in $\overline{\mathbb{K}(T)}[\underline{X}]$
where T is a variable.

Lemma 6 is an application of the well-known result of Bertini-Krull (see [24] theorem 37, p. 217 and corollary 1 p. 220). See also [21] chapitre 1, théorème fondamental for a precise statement and a direct proof.

Proof of theorem 2. The polynomial $\tilde{f}(X,Y)$ is indecomposable over $\mathbb{L}$ if and only if $\tilde{f}(X,Y)-T$ is irreducible in $\overline{\mathbb{L}(T)}[X,Y]$, by lemma 6. This condition holds, if and only if $f(\underline{X})-T$ is irreducible in $\overline{\mathbb{K}(T)}[\underline{X}]$, by lemma 5 which is true if and only if f is indecomposable over $\mathbb{K}$, by lemma 6. □

Theorem 3. *There exists a finite set of polynomials*

$$\Phi_t \in \mathbb{Z}[\ldots, b_{e_1,\ldots,e_n}, \ldots] =: \mathbb{E},$$

where the $b_{e_1,\ldots,e_n}$ *are variables, so that*
$\Phi_t(\ldots, c_{e_1,\ldots,e_n}, \ldots) = 0$ *for all* $t \iff f$ *is decomposable over* $\mathbb{K}$ *or* $\deg(f) < d$.
If $\mathbb{K}$ *has positive characteristic* $p > d^2/d_{min}$, *the coefficients of* Φ_t *are to be taken modulo* p *in the left-side equality.*
Furthermore, for all t,
$\deg(\Phi_t) \leq \frac{1}{2}(\frac{d}{d_{min}}+1)(\frac{d}{d_{min}}+2) := \mathcal{B}$.

Remarks:

(1) This theorem is similar to the classical Noether's theorem about 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 21. But when we study the absolute factorization of such a polynomial the degree of the Noether's absolute irreducibility forms are equal to $d^2 - 1 = 99$.

(2) We can get Theorem 3 without any hypothesis about p, but in this case the bound $\mathcal{B}$ is bigger. Indeed by lemma 6 f is decomposable if and only if $f-T$ is reducible in $\overline{\mathbb{K}(T)}[\underline{X}]$. Let Ψ_t be Noether's irreducibility forms associated to the polynomials of degree d, see [15] Theorem 7 for an effective statement about Ψ_t. By definition the family Ψ_t satisfies: $\forall t, \Psi_t(f) = 0 \iff f(\underline{X})$ is reducible over $\overline{\mathbb{K}}$ or $\deg f < d$.
Now we consider $\chi_t(T) = \Psi_t(f-T) \in \mathbb{K}[T]$. If all the coefficients of χ_t are equal to zero then $f-T$ is reducible over $\overline{\mathbb{K}(T)}$. Thus the coefficients of χ_t have the same property as Φ_t in Theorem 3. Unfortunately, the best bound known for the degree of Noether's irreducibility forms is $\deg \Psi_t \leq 12d^6$, see [15]. If we suppose that $p > d^2$ then we have $\deg \Psi_t \leq d^2 - 1$ see [23, 24]. That's why we use another strategy for our proof in order to have a good bound for $\deg \Phi_t$.

Now we prove Theorem 3. We use the bivariate statement of Theorem 1 (i.e. corollary 1) in order to get a sharp bound. A direct use of Theorem 1 for a polynomial with n variables gives

$\deg(\Phi_t) = O(d^n)$, where O is the Landau's notation.

Proof. We set following notation:

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

If we rewrite the proof of theorem 3 in [16] with the matrix $Jac_{\tilde{f}}$ instead of the Ruppert's matrix we then get:
The set of indecomposability forms is:

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

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 $Jac_{\tilde{f}}$ we have the desired result. □

Now we are going to give a probabilistic corollary of theorem 3. This corollary is based on the following lemma (see [29], [25]).

Lemma 7. *(Zippel-Schwartz) Let $P \in A[\underline{X}]$ be a polynomial of total degree d, where A is an integral domain. Let S be a finite subset of A. For a uniform random choice of x_i in S we have*

$$\mathcal{P}\Big(\{P(\underline{x}) = 0 \mid x_i \in S\}\Big) \leq d/|S|,$$

where $|S|$ is the cardinal of S.

Corollary 2. *Let $f(X_1, \dots, X_n) = \sum_{i_1+\dots+i_n\leq d} c_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n} \in \mathbb{K}[X_1, \dots, X_n]$, S be a finite subset of $\mathbb{K}$, and $p = 0$ or $p > d^2/d_{min}$.*
For a uniform random choice of $c_{i_1,\dots,i_n}$ in S we have:

$$\mathcal{P}\Big(\{f \text{ is indecomposable and } \deg f = d \mid c_{i_1,\dots,i_n} \in S\}\Big) \geq 1 - \mathcal{B}/|S|.$$

Proof. If f is decomposable or $\deg f < d$ then for all t we have $\Phi_t(c_{i_1,\dots,i_n}) = 0$. As $\cap_{t=1}^{r}\big(\Phi_t(c_{i_1,\dots,i_n}) = 0\big) \subset \Phi_1(c_{i_1,\dots,i_n}) = 0$, with the help of Lemma 7 and Theorem 3 we can conclude. □

Now we show with the help of Theorem 3 how we can reduce the study of a multivariate polynomial to the study of a bivariate one.

Theorem 4. *Let $\mathbb{K}$ be any field and S a finite subset of $\mathbb{K}$. Let $f \in \mathbb{K}[\underline{X}]$ be an indecomposable polynomial of total degree d. Suppose $\mathbb{K}$ has either characteristic zero or characteristic larger than d^2/d_{min}. For random choices of u_i's, v_i's and w_i's in S, with probability at least $1 - d.\mathcal{B}/|S|$ the polynomial $\overline{f}$ is indecomposable, where*

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

Proof. We want to show that

$$\mathcal{P}\Big(\{\overline{f} \text{ is indecomposable } \mid f \text{ is indecomposable and } \underline{u},\underline{v},\underline{w} \in S\}\Big) \geq 1 - d.\mathcal{B}/|S|.$$

In this proof, we will use the notations of Theorem 2, and we set:

$$\tilde{f}(X,Y) = \sum_{i,j} c_{i,j}(\underline{U},\underline{V},\underline{W})X^iY^j, \text{ with } c_{i,j}(\underline{U},\underline{V},\underline{W}) \in \mathbb{K}[\underline{U},\underline{V},\underline{W}].$$

By Theorem 3 we have:

$$\tilde{f} \text{ is decomposable } \iff \forall t, \Phi_t(c_{i,j}(\underline{U},\underline{V},\underline{W})) = 0.$$

We denote by $\Psi_t(\underline{U},\underline{V},\underline{W})$ the polynomial $\Phi_t(c_{i,j}(\underline{U},\underline{V},\underline{W}))$. We have $\deg \Psi_t \leq d.\mathcal{B}$, (it is enough to notice that each $c_{i,j}$ has at most degree d). This gives:

$$\tilde{f} \text{ is decomposable } \iff \forall t, \Psi_t(\underline{U},\underline{V},\underline{W}) = 0 \text{ in } \mathbb{K}[\underline{U},\underline{V},\underline{W}].$$

Thus

$$\deg(\overline{f}) < \deg(f) \text{ or } \overline{f} \text{ is decomposable } \iff \forall t, \Psi_t(\underline{u},\underline{v},\underline{w}) = 0 \text{ in } \mathbb{K}.$$

Then as in the proof of corollary 2 we get the desired result. □

Remark: We cannot obtain the same result if we use a substitution of this kind: $X_i = x_i$, for $i = 2,\ldots,n$. For example if we consider the polynomial $f(X_1,X_2,X_3) = X_1^6X_2^{10}X_3^{15}$ we have f is indecomposable. (Indeed, if we write $f = u(h)$ then $\deg(u)$ divides $gcd(6,10,15) = 1$, this remark will be generalized in the next section.) But for all $x \in \mathbb{K}$ we have $f(x,X_2,X_3)$, $f(X_1,x,X_3)$, $f(X_1,X_2,x)$ decomposable.

Now we study the evaluation of a parameterized polynomial. This case occurs when the field is of the form $\mathbb{K}(T_1,\ldots,T_m)$.

Theorem 5. *Let $\mathbb{K}$ be a field and S a finite subset of $\mathbb{K}$. Let*

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

be an indecomposable polynomial over $\mathbb{K}(T_1,\ldots,T_m)$ of total degree d. We supppose that $0 < \max(\deg a_{\underline{e}}) \leq \mathfrak{D}$ and that $\mathbb{K}$ has either characteristic zero or characteristic larger than d^2/d_{min}. For random choices of τ_i's in S, with probability at least $1 - \mathfrak{D}.\mathcal{B}/|S|$ the polynomial $f_{\underline{\tau}}(\underline{X}) = f(\tau_1,\ldots,\tau_m,\underline{X})$ is indecomposable over $\mathbb{K}$ and $\deg f = \deg f_{\underline{\tau}}$.

Proof. f is indecomposable then by Theorem 3, we have $\Phi_t\big(a_{\underline{e}}(\underline{T})\big) = P_t(\underline{T}) \neq 0$, where $\deg P(\underline{T}) \leq \mathfrak{D}.\mathcal{B}$. Bad cases appear when for all t we have $P_t(\underline{\tau}) = 0$. Thus we get the conclusion using Zippel-Schwartz's lemma as in corollary 2. □

4. Newton's polygon and Ostrowski's like theorem

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

Definition 4. *The support of $f(\underline{X})$ is the set S_f of integer points $(i_1, \ldots, i_n)$ 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 $S_f \cup \{(0, \ldots, 0)\}$. This set $N(f)$ is called the Newton's polygon of f.

Remark:
In other words $N(f)$ is the Newton's polygon of $f+\lambda$ where $\lambda \in \mathbb{K}$ is such that $f(0, \ldots, 0)+\lambda \neq 0$.

The next result is a necessary condition on the vertices of $N(f)$ when f is a decomposable polynomial. As we have f decomposable if and only if $f + \lambda$ is decomposable we have to take the origin with S_f when we compute the convex hull.

Proposition 1. *Let $f, h \in \mathbb{K}[\underline{X}]$, and $u \in \mathbb{K}[T]$ such that $f = u \circ h$.*
If $(i_1, \ldots, i_n)$ is a vertex of $N(f)$ then we can write $(i_1, \ldots, i_n) = (r.j_1, \ldots, r.j_n)$ where $r = \deg(u)$ and $(j_1, \ldots, j_n)$ is a vertex of $N(h)$.

Proof. First we remark that we can restrict our study to the case $f(0, \ldots, 0) \neq 0$. Indeed as we have already remarked, f is decomposable if and only if $f + \lambda$ is decomposable for any $\lambda \in \mathbb{K}$. Now we just have to remark that $f = u \circ h$ 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 $h(0, \ldots, 0) = 0$.
Thus $N(f) = \sum_{k=1}^{r} N(h - u_k)$ where the sum is the Minkowski sum of two convex sets. As the constant term of $h - u_k$ is not zero, all the $h - u_k$ have the same support. This gives $N(f) = rN(h - u_1)$. □

Definition 5. *Let $f \in \mathbb{K}[\underline{X}]$, $D = \gcd(i_1^{(1)}, \ldots, i_n^{(1)}, \ldots, i_1^{(k)}, \ldots, i_n^{(k)})$ where $(i_1^{(\alpha)}, \ldots, i_n^{(\alpha)})$ 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 $(\frac{i_1^{(\alpha)}}{D_{min}}, \ldots, \frac{i_n^{(\alpha)}}{D_{min}})$.
We denote by $\mathcal{E}$ the following set:
$\mathcal{E} = \{P(\underline{X}) \in \mathbb{K}[\underline{X}] \mid S_P \subset N(f)_{D_{min}}$ *and* $P(0, \ldots, 0) = 0\}$.

4.2. **Uni-multivariate decomposition modulo p.**

Now we give an Ostrowski like theorem for the uni-multivariate decomposition of integer bivariate polynomials. In the following theorem $\mathbb{F}_p$ is the field with p elements.

Theorem 6. *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 to say $H(f) = \max_{i,j} |c_{i,j}|$.
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:
$p > \max\left[\frac{d^2}{d_{min}}, \left(\frac{d^2}{D_{min}}\|f\|_2\right)^{T'}\right]$, *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 1:
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 1 this means that $f \mod p$ is indecomposable.
If $D \neq 1$ we follow the same strategy as in [11].
First we remark that we can restrict Jac_f to $\mathcal{E}$ and as $p > d^2/d_{min}$ we get:

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

(It suffices to rewrite corollary 1 with only two variables with the help of proposition 1.)
Now we just have to show that the dimension of the kernel remains equal to zero after the reduction $f \mod p$.
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 $\det M$ with the help of Hadamard's inequality. Each column of $Jac_{f/\mathcal{E}}$ corresponds to a polynomial of the following form: $[f, X^aY^b] = (\partial_X f)bX^aY^{b-1} - (\partial_Y f)aX^{a-1}Y^b$, where $(a,b) \in N(f)_{D_{min}}$. Thus a, b are smaller than d/D_{min}. Moreover $[f, X^aY^b] = \sum_{i,j}(ib - aj)c_{i,j}X^{a+i-1}Y^{b+j-1}$, where i and j are smaller than d. Then each column has a norm smaller than $\dfrac{d^2}{D_{min}}\|f\|_2$. Hence Hadamard's inequality gives:

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

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 $Jac_{f \mod p/\mathcal{E}}$.
Then when $p > \max\Big[d^2, \Big(\dfrac{d^2}{D_{min}}\|f\|_2\Big)^{T'}\Big]$, $Jac_{f \mod p/\mathcal{E}}$ has full rank, and we can apply property $(\star)$. Thus $f \mod p$ is indecomposable. □

5. An indecomposability test

In a generic situation a polynomial is indecomposable. Then in order to have an efficent algorithm in practice we must have a quick indecomposability test. That is to say before looking for a decomposition we test if the polynomial is indecomposable or not. Our test is a direct corollary of Proposition 1 and this idea has already been used for Theorem 6. A similar test for the absolute factorization has already been studied in [4], chapitre 5.

Corollary 3. *Let* $(i_1^{(1)}, \ldots, i_n^{(1)}, \ldots, i_1^{(k)}, \ldots, i_n^{(k)})$ *be the vertices of* $N(f)$.
If $\gcd(i_1^{(1)}, \ldots, i_n^{(1)}, \ldots, i_1^{(k)}, \ldots, i_n^{(k)}) = 1$ *then* f *is indecomposable.*

Remark: If we do not take the origin with the support then this corollary 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 $S_f = \{(2,1), (8,4), (10,10), (5,5)\}$ and $\gcd(1,2,8,4,10,5) = 1$.

Thus we have a test to check the indecomposability of a polynomial. If the polynomial f is dense, then the coordinates of the vertices of $N(f)$ are $(0,\dots,0)$, $(d,0,\dots,0)$, $(0,\dots,d)$. In this case our test return: "I don't know". However if the polynomial f is sparse then with Corollary 3 we can often quickly detect if f is indecomposable. The following table gathers some statistic evidences about this claim. This test has been implemented in MAGMA [19], and is freely available at http://www.mip.ups-tlse.fr/∼cheze/.

d	$Sparse$	$Success$	T_{moy}	T_{max}	T_{min}
10	0	0	0.00015	0.011	0
10	1	711	0.00007	0.011	0
10	2	837	0.00009	0.011	0
10	10	914	0.0009	0.011	0
100	2	836	0.013	0.021	0
200	2	848	0.1821	0.23	0.13

We have constructed randomly 1000 polynomials of total degree d with two variables. $Sparse$ is the number of coefficients equal to zero divided by the number of nonzero coefficients. Then $Sparse = 0$ means "the polynomial is dense", $Sparse = 1$ means that one half of the coefficients are equal to zero. The coefficients of f belong to $[-10^{12}; 10^{12}]$. $Success$ is the number of indecomposable polynomials detected with our test. T_{moy} (respectively T_{max}, T_{min}) is the average (respectively the maximum, the minimum) timing in seconds to do one test.
This table shows that our test is well suited for sparse polynomial.

5.1. **The Newton's polygon test with a modular strategy.** We have good results for sparse polynomials, so in the following the idea is to "transform" a dense polynomial into a "sparse" one, that is to say we are going to "break" the Newton polytope.

Proposition 2. *Let* $f(X,Y) \in \mathbb{Z}[X,Y]$ *and* $f(X,Y) \bmod p \in \mathbb{F}_p[X,Y]$. *If* $\deg(f) = \deg(f \bmod p)$ *and* $f \bmod p$ *is indecomposable, then* f *is indecomposable.*

Proof. To prove this we show: f is decomposable implies $f \bmod p$ is decomposable.
If f is decomposable then $f = u \circ h$ with $\deg u \geq 2$.
Furthermore we have $f \bmod p = (u \bmod p) \circ (h \bmod p)$ and then:
$\deg(u \bmod p)\deg(h \bmod p) = \deg(f \bmod p) = \deg(f) = \deg u \deg h$.
Hence $\deg(u \bmod p) \geq 2$ because $\deg(h \bmod p) \leq \deg h$. □

Now, the idea is to study $f \bmod p$ instead of f, because even if f is dense $f \bmod p$ may be sparse.
Let $a_1,\dots,a_k$ be the coefficients corresponding to the vertices of $N(f)$ and $L = [p_1,\dots,p_l]$ be the list of the primes dividing at least one of the a_i. We remark:

$$\forall p_i \in L,\ N(f) \neq N(f \bmod p_i).$$

So we can test the decomposability of f with this Las Vegas strategy (the algorithm is probably fast, and the output is always correct but it is possible to get the output: "I don't know"):

Modular Indecomposability test:
INPUT: $f \in \mathbb{Z}[X,Y]$.
For each $p \in L$, test the decomposability of $f \mod p \in \mathbb{F}_p[X,Y]$ with the help of the Newton's polygon (see corollary 3), and conclude with proposition 2.
If $f \mod p$ don't satisfy corollary 3 for all $p \in L$ then return "I don't know".

This test has been implemented in MAGMA [19], and is freely available at http://www.mip.ups-tlse.fr/∼cheze/.

The following table shows some results obtained with this algorithm. We have constructed 1000 polynomials in $\mathbb{Z}[X,Y]$ of total degree d, with random integer coefficients in $[-10^{12}; 10^{12}]$. All these polynomials are dense. For each polynomial we test its decomposability with the previous algorithm. *Success* is the number of indecomposable polynomials detected with this algorithm. T_{moy} (respectively T_{max}, T_{min}) is the average (respectively the maximum, the minimum) timing in seconds to do one test.

d	*Success*	T_{moy}	T_{max}	T_{min}
10	1000	0.002	0.011	0
30	1000	0.002	0.011	0
50	1000	0.013	0.06	0
100	1000	0.171	0.63	0.139
200	1000	2.581	9.451	2.16

Remarks:

(1) This algorithm is efficient even if we have dense random polynomials.
(2) The drawback of our method appears when we study polynomial like $f(X,Y) = X^d + Y^d + 1$. Indeed in this case the Newton polygon gives no information, even if we look at $f \mod p$. Now, the idea is to use a change of coordinates of the following type $f(aX + bY, cX + dY)$ in order to obtain a polynomial with new coefficients.
(3) In what precedes, we only considered the case of integer polynomials. However our tests can be extended to the case of polynomials with coefficients in a commutative ring. In this case, the computation modulo a prime number will be substituted by a computation modulo a prime ideal.
(4) When the number of variables n increases the probability of success must increase with n. Indeed, when a polynomial has n variables each vertex of the Newton polygon has n coordinates. Then we have more coordinates and thus more chances to obtain a gcd equal to 1. Our implementation relies on the Magma's function: *NewtonPolygon*. Unfortunately

this function works only for bivariate polynomials, that's why our tables show numerical evidences only for bivariate polynomials.

By corollary 2, f is indecomposable with a probability larger than: $1 - 10^{-11}$. Thus it is not surprising to always get indecomposable polynomials. But it is not obvious that the Modular Indecomposability test always return: "True". So a question is open. If we set:
$\mathcal{F} = \{f \mid c_{i,j} \in S$ and $Modular\, Indecomposability\, test(f) =$ "I don't know"$\}$.
What is the probability $\mathcal{P}(\{$ f is indecomposable $\mid c_{i,j} \in S\} \cap \mathcal{F})$?

Acknowledgments

The authors thank Arnaud Bodin, Pierre Dèbes, and Grégoire Lecerf for their precious comments. During the preparation of this paper, the second author was supported by the Abdus Salam International Centre for Theoretical Physics, Trieste, Italy; for this he wishes to thank Lê Dung Tráng and all staff for their encouragement.

References

[1] I. V. Arzhantsev and A.P. Petravchuk, *Closed and Irreducible Polynomials in Several Variables*, arXiv:math/0608157v2, 20 May 2007.
[2] 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.
[3] A. Bodin, P. Dèbes, S. Najib, ..., Work in progress.
[4] 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).
[5] G. Chèze, *Approximate uni-multivariate decomposition of bivariate polynomials with a jacobian matrix*, Work in progress.
[6] G. Chèze, G. Lecerf, *Lifting and Recombination Techniques for Absolute Factorization*, Journal of Complexity (2007), 23 (3), 380–420.
[7] G. Chèze, G. Lecerf, *A uni-multivariate decomposition algorithm*, Work in progress.
[8] E. Cygan, *Factorization of polynomials*, Bull. Polish Acad. Sci. Math. 40 (1992), 45–52.
[9] M. Fried, R.E.Mac Rae, *On the invariance of chains of fields*, Illinois J. Math. 13 (1969), 165–171.
[10] S. Gao, *Factoring multivariate polynomials via partial differential equations*, Math. Comp. 72 (2003), 801–822.
[11] S. Gao, V. Rodrigues, *Irreducibility of polynomials modulo p via Newton polytopes*, J. Number Theory, 101 (2003), 32–47.
[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] D. Lorenzini, *Reducibility of polynomials in two variables*, J. Algebra 156 (1993), 65–75.
[19] 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.
[20] S. Najib, *Une généralisation de l'inégalité de Stein-Lorenzini*, J. Algebra 292 (2005), 566–573.
[21] S. Najib, *Factorisation des polynômes $P(X_1, \ldots, X_n) - \lambda$ et théorème de Stein*, Thèse de Doctorat. Univ. Lille 1 (2005).
[22] W. M. Ruppert, *Reducibility of polynomials $f(x,y)$ modulo p*, J. Number Theory, 77 (1999) 62–70.
[23] W. M. Ruppert, *Reduzibilität ebener Kurven*, J. Reine Angew. Math. 369 (1986), 167–191.

[24] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, 77. Cambridge University, 2000.
[25] J.T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. Assoc. Comput. Mach. 27 (1980), 701–717.
[26] Y. Stein, *The total reducibility order of a polynomial in two variables*, Israel J. Math. 68 (1989), 109–122.
[27] Joachim von zur Gathen. Functional decomposition of polynomials: the tame case. *J. Symbolic Comput.*, 9(3):281–299, 1990.
[28] J. von zur Gathen, J. Gutierrez, R. Rubio, *Multivariate polynomial decomposition*, Appl. Algebra Engrg. Comm. Comput. 14 (2003), 11–31.
[29] R. E. Zippel, *Effective polynomial computation*, Boston: Kluwer Academic Press, 1993.