Article Submitted to Journal of Symbolic Computation

From an approximate to an exact absolute polynomial factorization

Guillaume Chèze[1] and André Galligo[1]

[1] *Laboratoire de mathématiques, Univerité de Nice Sophia Antipolis, Parc Valrose, Nice 06108 Cedex 2*

E-mail: `cheze@math.unice.fr, galligo@math.unice.fr`

Abstract

We propose an algorithm to compute an exact absolute factorization of a bivariate polynomial from an approximate one. This algorithm is based on some properties of the algebraic integers over $\mathbb{Z}$ and is certified. It relies on a study of the perturbations in a Vandermonde system. We provide a sufficient condition on the precision of the approximate factors, depending only on the height and the degree of the polynomial.

1. Introduction

The aim of this article is to provide a rigorous and efficient treatment of a major step in the factorization algorithms which proceed via approximations e.g. [8], [5], [14], [17], [20], [9], [2], [3]. For the study of approximate irreducibility and approximate factorization, one can see [11] and [10].
We consider an irreducible polynomial $P \in \mathbb{Q}[X,Y]$ and denote by $P = P_1 \cdots P_s$ the factorization of P in $\mathbb{C}[X,Y]$, where P_i is irreducible in $\mathbb{C}[X,Y]$. We call this factorization the absolute factorization of P.

Let $\mathbb{Q}[\alpha]$ be the smallest extension of $\mathbb{Q}$ which contains all the coefficients of the factor P_1. Let $P \approx \tilde{P}_1 \cdots \tilde{P}_s$ be an approximate absolute factorization of P. By this we mean that $\tilde{P}_i \in \mathbb{C}[X,Y]$ and the coefficients of $\tilde{P}_i$ are numerical approximations of the coefficients of P_i with a given precision ϵ. That is to say $\|P_i - \tilde{P}_i\|_\infty < \epsilon$ with respect to the norm $\| \sum_{i,j} a_{i,j} X^i Y^j \|_\infty = \max_{i,j} |a_{i,j}|$. The norm $\|P\|_\infty$ is called the height of P.

A natural question is: Can we get an exact factorization from an approximate one? If it is possible: how can we find the minimal polynomial of α over $\mathbb{Q}$, and how can we express the coefficients of P_1 in $\mathbb{Q}[\alpha]$?

We will answer positively if ϵ is small enough. As the coefficients of $\tilde{P}_1$ are given with an error ϵ, in order to find the minimal polynomial f_α of α, ($f_\alpha \in \mathbb{Q}[T]$), we have to recognize its coefficients which are rational numbers from floating points approximations. David Rupprecht gave a preliminary study of this problem in [14], and [15]. Here we present a complete and satisfactory answer.

1.1. Notations and elementary results

P belongs to $\mathbb{Q}[X,Y]$ and $P = P_1 \cdots P_s$ in $\mathbb{C}[X,Y]$. Each P_i is an irreducible factor of P in $\mathbb{C}[X,Y]$. $\mathbb{K}$ is the smallest field which contains all the coefficients of P_1, $\mathbb{K}$ is a finite extension of $\mathbb{Q}$. By the primitive element theorem we can write $\mathbb{K} = \mathbb{Q}[\alpha]$. Let $x \in \mathbb{K}$, we denote by f_x the minimal polynomial of x over $\mathbb{Q}$. We recall that f_x is monic. $\mathcal{O}_{\mathbb{K}}$ is the ring of algebraic integers in $\mathbb{K}$: If $x \in \mathcal{O}_{\mathbb{K}}$ then $f_x(T) \in \mathbb{Z}[T]$.

Let $x \neq 0$ be an element of $\mathbb{K}$, we denote by m_x the homomorphism of multiplication by x in $\mathbb{K}$ and by $P_{char}(x)$ the characteristic polynomial of m_x, similarly, $Tr_{\mathbb{K}/\mathbb{Q}}(x)$ is the trace of m_x. We recall that $P_{char}(x) = f_x^k$ where $k = [\mathbb{K} : \mathbb{Q}[x]]$ is the degree of $\mathbb{K}$ over $\mathbb{Q}[x]$.

As usual, we also denote by lc the leading coefficient of a univariate polynomial, and by $\mathcal{M}_{m,n}(\mathbb{C})$ the ring of matrices with m rows and n columns, with coefficients in $\mathbb{C}$.

1.2. Our strategy

First we recall a lemma which implies a strong property on the factor P_i of P.

Lemma 1.1 (Fundamental Lemma): *Let $P \in \mathbb{Q}[X,Y]$ be an irreducible polynomial in $\mathbb{Q}[X,Y]$, monic in Y.*
$P(X,Y) = Y^n + a_{n-1}(X)Y^{n-1} + \cdots + a_0(X)$ *with* $deg(a_i(X)) \leq n-i$.
Let $P = P_1 \cdots P_s$ be a factorization of P by irreducible polynomials P_i in $\mathbb{C}[X,Y]$. Denote by $\mathbb{K} = \mathbb{Q}[\alpha]$ the extension of $\mathbb{Q}$ generated by all the coefficients of P_1. Then each P_i can be written:
$P_i(X,Y) = Y^m + b_{m-1}(\alpha_i, X)Y^{m-1} + \cdots + b_0(\alpha_i, X)$, *with* $b_k \in \mathbb{Q}[Z,X]$, $deg_X(b_k) \leq m-k$, *and where $\alpha_1, \ldots, \alpha_s$ are the different conjugates over $\mathbb{Q}$ of $\alpha = \alpha_1$.*

See [15][lemma 2.2] for a proof.
As a corollary the number of absolute factors is equal to $[\mathbb{K} : \mathbb{Q}]$.
Our aim is to compute the minimal polynomial of α where α is a primitive element of $\mathbb{K}$ and then the coefficients of P_1 in $\mathbb{K}$. Our strategy is based on the following observations.
Let $P_i(X,Y) = \sum_u \sum_v a_i^{(u,v)} X^u Y^v$ then we have (by the fundamental lemma):

$$P_{char}(a_1^{(u,v)})(T) = \prod_{i=1}^{s} (T - a_i^{(u,v)}) = T^s + c_{s-1}T^{s-1} + \cdots + c_0.$$

Theoretically, to check if such a $P_{char}(a)$ is the minimal polynomial of a over $\mathbb{Q}$, we just have to compute the gcd of $P_{char}(a)$ and $\frac{\partial}{\partial T}P_{char}(a)$, see lemma 3.1. However in our situation, we do not have exact data $a_1^{(u,v)}, \ldots, a_s^{(u,v)}$, but only approximations $a_1^{(u,v)}+\epsilon_1, \ldots, a_s^{(u,v)}+\epsilon_s$ and a bound ϵ, on the errors ϵ_i. Expanding $\prod_{i=1}^s(T-a_i^{(u,v)}-\epsilon_i)$, we get $T^s+c_{s-1}(\epsilon)T^{s-1}+\cdots+c_0(\epsilon)$, therefore we need to recognize c_i from $c_i(\epsilon)$. Without a bound on the denominators of the rational numbers c_i, this might be tough.

In order to avoid this difficulty, we show in section 2 that we can restrict our study to a polynomial $P(X,Y)\in\mathbb{Z}[X,Y]$. Then we prove that the coefficients of P_i are algebraic integers over $\mathbb{Z}$. Therefore, the coefficients of the minimal polynomial will be integers. In section 3 we show how to recognize them and certify the result. In Section 4 we propose a certified algorithm to obtain the expression of the coefficients of P_1 in $\mathbb{K}$. We rely on the fundamental lemma and an adapted representations of these algebraic integers over $\mathbb{Z}$.

2. A tool-bag

2.1. Reduction to $\mathbb{Z}[X,Y]$

Let $Q(X,Y)=\sum_{i=0}^n\sum_{j=0}^i q_{j,n-i}X^jY^{n-i}$ be an irreducible and monic polynomial in $\mathbb{Q}[X,Y]$ of total degree n. Let d be a common denominator of the coefficients of Q that is to say $dq_{j,n-i}\in\mathbb{Z}$. Then d^nQ is irreducible in $\mathbb{Q}[X,Y]$ and $d^nQ(X,Y)=\sum_{i=0}^n\sum_{j=0}^i d^iq_{j,n-i}X^j(dY)^{n-i}$. Setting $Z=dY$ we define:
$d^nQ(X,Y)=d^nQ\left(X,\frac{Z}{d}\right)=Z^n+dq_{1,n-1}XZ^{n-1}+\cdots+d^nq_{0,0}=P(X,Z)$.

Since $d^nQ(X,Y)$ is irreducible in $\mathbb{Q}[X,Y]$, $d^nQ(X,\frac{Z}{d})$ is irreducible in $\mathbb{Q}[X,Z]$ hence $P(X,Z)$ is monic, irreducible in $\mathbb{Q}[X,Z]$ and belongs to $\mathbb{Z}[X,Z]$. We now state two lemmas whose proofs are obvious.

Lemma 2.1: *Let $Q(X,Y)$ be a polynomial satisfying the hypotheses of the fundamental lemma; d a common denominator of the coefficients of Q and $Q(X,Y)=Q_1(X,Y)\cdots Q_s(X,Y)$ its absolute factorization in $\mathbb{C}[X,Y]$. Then $P(X,Y)=d^nQ\left(X,\frac{Y}{d}\right)=d^mQ_1\left(X,\frac{Y}{d}\right)\cdots d^mQ_s\left(X,\frac{Y}{d}\right)$, $P(X,Y)\in\mathbb{Z}[X,Y]$ is irreducible in $\mathbb{Q}[X,Y]$ and monic relatively to Y, and $P_i(X,Y)=d^mQ_i\left(X,\frac{Y}{d}\right)$ are the irreducible factors of P in $\mathbb{C}[X,Y]$.*

Lemma 2.2: *Let $\mathbb{K}'$ be the subfield of $\mathbb{C}$ generated by the coefficients of Q_1 and $\mathbb{K}$ the smallest field generated by the coefficients of P_1, then $\mathbb{K}'=\mathbb{K}$.*

From now on, we suppose that our input polynomial belongs to $\mathbb{Z}[X,Y]$.

2.2. The coefficients of P_i are algebraic integers over $\mathbb{Z}$

Here we prove first a lemma then the following theorem.

THEOREM 2.1: *Let $P \in \mathbb{Z}[X,Y]$ be monic and irreducible in $\mathbb{Q}[X,Y]$. Then, it admits a factorization in $\mathbb{C}[X,Y]$: $P_1 \cdots P_s$ which consists of absolute irreducible polynomials whose coefficients are algebraic integers over $\mathbb{Z}$.*

LEMMA 2.3: *Let α be an algebraic number over $\mathbb{Q}$ and $p(X) \in \mathbb{Q}[\alpha][X]$ be an integer over $\mathbb{Z}[X]$. Then all the coefficients of $p(X)$ are integers over $\mathbb{Z}$.*

Proof: We denote by s the degree of α over $\mathbb{Q}$ and by l the degree of p in X. Then $\mathbb{Q}(X)[\alpha]$ is an extension of $\mathbb{Q}(X)$ of degree s. Moreover:

$(*)$ All the conjugates of $p(X)$ over $\mathbb{Q}(X)$ belong to $\mathbb{C}[X]$ and have the same degree l.

As $\mathbb{Z}[X]$ is an integrally closed ring we deduce (see e.g.[16] p.45) that:

$(**)$ The coefficients of the characteristic polynomial $P_{char}(p(X))$ of $p(X)$ over $\mathbb{Q}(X)$ are in $\mathbb{Z}[X]$.

Let $k = [\mathbb{Q}(X)[\alpha] : \mathbb{Q}(X)[p(X)]]$, we denote the conjugates of $p(X)$ over $\mathbb{Q}(X)$ by q_i for $i = 1, \dots, s/k$ and $q_1 = p(X)$, then $P_{char}(p(X))(Z) = \prod_{i=1}^{s/k}(Z - q_i)^k$ is the characteristic polynomial of $p(X)$.

Now we prove by induction that all the coefficients of $p(X)$ are integers over $\mathbb{Z}$. We start by the leading term of $p(X)$. We have:

$$P_{char}(p(X))(Z) = Z^s + (\sum_i q_i)Z^{s-1} + \dots + \prod_i q_i = Z^s + c_{s-1}(X)Z^{s-1} + \dots + c_0(X),$$

with $c_i(X) \in \mathbb{Z}[X]$ by $(**)$, and $deg(c_{s-i}(X)) \leq il$, by $(*)$.
Thus $deg(c_{s-i}(X)p(X)^{s-i}) \leq ls$.

As $P_{char}(p(X))(p(X)) = 0$ in $\mathbb{C}[X]$, the term of degree ls gives:

$$\lambda_l^s + \sum_{i \in I} \mathrm{lc}(c_{s-i})\lambda_l^{s-i} = 0,$$

where $\lambda_l = \mathrm{lc}(p(X))$ and I is the set $I = \{i \mid deg(c_{s-i}(X)p(X)^{s-i}) = ls\}$.

The fact that all $\mathrm{lc}(c_i)$ are integers, implies that λ_l is an algebraic integer over $\mathbb{Z}$ therefore $\lambda_l X^l$ is an algebraic integer over $\mathbb{Z}[X]$.

To prove the other steps of the induction, we simply remark that $p(X) - \lambda_l X^l$ belongs to $\mathbb{Q}[\alpha][X]$ and is an integer over $\mathbb{Z}[X]$, then we can repeat the previous argumentation with $p(X) - \lambda_l X^l$, instead of $p(X)$. □

Now we prove the theorem.

Proof: As in the previous section, $\mathbb{K} = \mathbb{Q}[\alpha]$ is the extension field generated by all the coefficients of P_1, and the degree of α over $\mathbb{Q}$ is s. By Steinitz's theorem, there exists an algebraically closed field $\mathcal{K}$ such that $\mathcal{K} \supset \mathbb{Q}(X) \supset \mathbb{Z}[X]$ and

$$P(X,Y) = Y^n + a_{n-1}(X)Y^{n-1} + \dots + a_0(X) = \prod_{i=1}^{n}(Y - r_i(X)),$$

where $r_i(X) \in \mathcal{K}$ are algebraic integers over $\mathbb{Z}[X]$. (see e.g. [6] p.300 corollary 13.16.)

As $P_1(X,Y)$ is a factor of $P(X,Y)$ in $\mathbb{Q}(\alpha)[X,Y]$, we have:

$$P_1(X,Y) = \prod_{i=1}^{m}(Y - r_i(X)) = Y^m + p_{m-1}(X)Y^{m-1} + \cdots + p_0(X).$$

Then $p_i(X)$ are integers over $\mathbb{Z}[X]$ because they are polynomials in $r_i(X)$. Applying the previous lemma to each $p_i(X)$ we deduce the claim. $\square$

3. Finding a primitive element

All the coefficients of P_1 generate an extension $\mathbb{K}$ of $\mathbb{Q}$. We want to get a primitive element of $\mathbb{K}$ which is an *algebraic integer over* $\mathbb{Z}$. There are two cases: First, we check if there is a primitive element among all the coefficients of P_1. If it is not the case, we present a method to construct a primitive element. (In our examples we always found a coefficient of P_1 which was a primitive element.)

3.1. Recognition

The followinng easy lemma allows us to recognize effectively a primitive element.

LEMMA 3.1: *Let $\beta \in \mathbb{K}$, we have:*

$$\gcd(P_{char}(\beta), \frac{\partial}{\partial T}P_{char}(\beta)) = 1 \iff \beta \textit{ is a primitive element of } \mathbb{K}.$$

In this case $P_{char}(\beta)$ is the minimal polynomial f_β of β over $\mathbb{Q}$.

Let $P_i(X,Y) = \sum_u \sum_v a_i^{(u,v)} X^u Y^v$, the fundamental lemma implies that: $P_{char}(a_1^{(u,v)})(T) = \prod_{i=1}^{s}(T - a_i^{(u,v)})$. Then:

$a_1^{(u,v)}$is a primitive element of $\mathbb{K}$ if and only if $\gcd(P_{char}(a_1^{(u,v)}), \frac{\partial}{\partial T}P_{char}(a_1^{(u,v)})) = 1.$

3.2. Construction

If no coefficient of P_1 is primitive, we construct with high probability a primitive element, which is integer over $\mathbb{Z}$. Thanks to lemma 3.1 we can check if this constructed element is primitive.

We denote by σ_i, $(1 \leq i \leq s)$ the s independent $\mathbb{Q}$-homomorphisms from $\mathbb{K}$ to $\mathbb{C}$ and by $a_1^{(u,v)}$ the coefficients of P_1, we recall that they generate $\mathbb{K}$.

For any pair (i,j) such that $i \neq j$, there exists a coefficient $a_1^{(u,v)}$ of P_1 such that $\sigma_i(a_1^{(u,v)}) \neq \sigma_j(a_1^{(u,v)})$. Thus the polynomial:

$$H(\lambda_{(0,0)},\dots,\lambda_{(2,m-1)}) = \prod_{i<j}\Big(\sum_{0\leq u+v\leq m} \lambda_{(u,v)}(\sigma_i-\sigma_j)\big(a_1^{(u,v)}\big)\Big) \in \mathbb{C}[\lambda_{(i,j)}]$$

is a non zero polynomial. So there exists $(s_{(0,0)},\dots,s_{(2,m-1)})$ with $s_{(u,v)} \in \mathbb{Z}$ such that for all $i \neq j$:

$$\sigma_i\Big(\sum_{0\leq u+v\leq m} s_{(u,v)}a_1^{(u,v)}\Big) \neq \sigma_j\Big(\sum_{0\leq u+v\leq m} s_{(u,v)}a_1^{(u,v)}\Big)$$

This means that $\sum_{0\leq u+v\leq m} s_{(u,v)}a_1^{(u,v)}$ is a primitive element.
The following probabilistic lemma [21], [19] helps us to conclude:

LEMMA 3.2: *Let A be an integral domain, $H(\lambda_1,\dots,\lambda_n) \in A[\lambda_1,\dots,\lambda_n]$ a non-zero polynomial of total degree d and S a subset of A. In this case we have the following bound on the probability:*

$$\mathcal{P}(H(s_1,\dots,s_n)=0 \mid s_i \in S,\, 1\leq i\leq n) \leq \frac{d}{|S|},$$

where s_i are chosen in S uniformly at random.

We apply this lemma to the polynomial $H(\lambda_{(0,0)},\dots,\lambda_{(2,m-1)}) \in \mathbb{C}[\lambda_{(i,j)}]$ and get the following proposition:

PROPOSITION 3.1: *Let P be a polynomial in $\mathbb{Z}[X,Y]$ monic and irreducible in $\mathbb{Q}[X,Y]$, $P = P_1\cdots P_s$ its irreducible decomposition in $\mathbb{C}[X,Y]$.
Let $a_1^{(u,v)}$ denote the coefficients of P_1, and $\mathbb{K}$ the extension of $\mathbb{Q}$ they generate.
Let S be a subset of $\mathbb{Z}$. Then we have the following estimation of probability:*

$$\mathcal{P}\big(\sum_{0\leq u+v\leq m} s_{(u,v)}a_1^{(u,v)} \text{ primitive} \mid s_{(u,v)} \in S\big) \geq 1 - \frac{\binom{s}{2}}{|S|},$$

where $s_{(u,v)}$ are chosen in S uniformly at random.

As the $a_1^{(u,v)}$ are integers over $\mathbb{Z}$, $\sum_{0\leq u+v\leq m} s_{(u,v)}a_1^{(u,v)}$ is an algebraic integer over $\mathbb{Z}$. Moreover we can check with lemma 3.1 if this element is primitive or not.

Remark: We can get a primitive element in a deterministic way, but in this case the coefficients $s_{(u,v)} \in \mathbb{Z}$ are bigger than the ones obtained with the probabilistic method, see [4].

3.3. A bound on the coefficients of the factors

Below, we will need a bound on $\|P_i\|_\infty$. We recall a classical result (see [18], [12]).

PROPOSITION 3.2: *Let $F_1, \dots, F_k \in \mathbb{C}[X,Y]$, we have:*

$$\prod_{i=1}^{k} \|F_i\|_\infty \leq 2^{\nu} \| \prod_{i=1}^{k} F_i \|_\infty$$

where $\nu = \sum_{i=1}^{k} \Big(\deg_X(F_i) + \deg_Y(F_i) \Big)$.

In our situation we get:

COROLLARY 3.1: *With our previous notations, we have:*

$$\|P_i\|_\infty \leq 2^{2n} \|P\|_\infty.$$

Proof: We apply proposition 3.2, and we use the facts that $n = sm$, and that P_i are monic in Y. □

There exists others bound on $\|P_i\|_\infty$, for example using formulae from [18], [12], we get: $\|P_i\|_\infty \leq 2^{2m}\|P\|_2$, where $\| \sum_{i,j} a_{i,j} X^i Y^j \|_2 = \sqrt{\sum_{i,j} a_{i,j}^2}$.
We conclude that we are able to bound the height of the factors in terms of the height of P and of the degree of P.

3.4. Choice of the precision

In practice with an approximate absolute factorization, we can only compute an approximation of a minimal polynomial $f_\alpha(T)$, which writes $f_{\tilde{\alpha}}(T) = \prod_{k=1}^{s}(T - (\alpha_k + \epsilon_k))$.

We have perturbed roots and we want to know if the perturbation on the coefficients is smaller than 0.5 in order to recognize the polynomial $f_\alpha(T) \in \mathbb{Z}[T]$ from $f_{\tilde{\alpha}}(T)$. The following map describes the situation:

$$\begin{array}{cccc}
\varphi : & \mathbb{C}^s & \longrightarrow & \mathbb{C}^s \\
& \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \\ \vdots \\ \alpha_s \end{pmatrix} & \longmapsto & \begin{pmatrix} S_1(\alpha_1, \dots, \alpha_s) & = & \alpha_1 + \alpha_2 + \cdots + \alpha_s \\ & \vdots & \\ S_k(\alpha_1, \dots, \alpha_s) & = & \displaystyle\sum_{1 \leq i_1 < \ldots < i_k \leq s} \alpha_{i_1} \cdots \alpha_{i_k} \\ & \vdots & \\ S_s(\alpha_1, \dots, \alpha_s) & = & \alpha_1 \times \cdots \times \alpha_s \end{pmatrix}
\end{array}$$

We define the norm $\|.\|_\infty$ by $\|(\alpha_1, \dots, \alpha_s)\|_\infty = \max_{i=1,\dots,s} |\alpha_i|$. We look for a condition on ϵ which will imply $\|\varphi(\alpha + \epsilon) - \varphi(\alpha)\|_\infty < 0.5$.

φ is a polynomial map such that the degree of each component is smaller or equal to s and is of degree 1 in each variable. With the following notation:

$$\left[\sum_{i=1}^{s}\epsilon_i\frac{\partial\varphi}{\partial\alpha_i}(\alpha)\right]^{[k]} = \sum_{\substack{i_1+\cdots+i_s=k\\ i_j\in\{0,1\}}}\frac{k!}{i_1!\dots i_s!}\epsilon_1^{i_1}\cdots\epsilon_s^{i_s}\frac{\partial^k\varphi}{\partial\alpha_1^{i_1}\cdots\partial\alpha_s^{i_s}}(\alpha),$$

the Taylor expansion of φ is:

$$\varphi(\alpha+\epsilon)-\varphi(\alpha) = \left[\sum_{i=1}^{s}\epsilon_i\frac{\partial\varphi}{\partial\alpha_i}(\alpha)\right]+\frac{1}{2!}\left[\sum_{i=1}^{s}\epsilon_i\frac{\partial\varphi}{\partial\alpha_i}(\alpha)\right]^{[2]}+\cdots+\frac{1}{s!}\left[\sum_{i=1}^{s}\epsilon_i\frac{\partial\varphi}{\partial\alpha_i}(\alpha)\right]^{[s]}$$

We introduce the constants ϵ_α and M_α such that:

- $|\alpha_i| \leq M_\alpha$ for all $1 \leq i \leq s$
- $|\epsilon_i| \leq \epsilon_\alpha < 1$.

Remark: If the primitive element α corresponds to a coefficient of P_1, we have:

$$|\alpha_i| \leq \|P_i\|_\infty \leq 2^{2n}\|P\|_\infty.$$

If the primitive elements α is a linear combination of some coefficients of P_1: $\alpha = \sum_{i,j}\lambda_{i,j}a_1^{(i,j)}$, then we have: $|\alpha| \leq \left(\sum_{i,j}|\lambda_{i,j}|\right)2^{2n}\|P\|_\infty$.
Thus we can bound M_α in terms of the height of P and its degree n. Now give a bound on ϵ_α, in order to get the exact minimal polynomial from the approximate one.

LEMMA 3.3: *With the previous notations, we have:*

$$\|\varphi(\alpha+\epsilon)-\varphi(\alpha)\|_\infty \leq \left(1+\sum_{k=1}^{s-1}\binom{s}{k}\max\left(1, \max_{j=k+1,\dots,s}\left(\binom{s-k}{j-k}M_\alpha^{j-k}\right)\right)\right)\epsilon$$

Proof: The total degree of the polynomial S_j is j, so we deduce:

- If $k > j$ then $\dfrac{\partial^k S_j}{\partial\alpha_1^{i_1}\cdots\partial\alpha_s^{i_s}}(\alpha) = 0$.
- If $k = j$ then $\dfrac{\partial^k S_j}{\partial\alpha_1^{i_1}\cdots\partial\alpha_s^{i_s}}(\alpha) = 1$.

Moreover, we get the following upper bound, for $k < j$:

$$\left|\frac{\partial^k S_j}{\partial\alpha_1^{i_1}\cdots\partial\alpha_s^{i_s}}(\alpha)\right| \leq \binom{s-k}{j-k}M_\alpha^{j-k}.$$

As a result we obtain:

$$\left\| \frac{\partial^k \varphi}{\partial \alpha_1^{i_1} \cdots \partial \alpha_s^{i_s}}(\alpha) \right\|_\infty \leq \max\left(1, \max_{j=k+1\cdots s}\left(\binom{s-k}{j-k} M_\alpha^{j-k}\right)\right).$$

It follows:

$$\left\| \left[\sum_{i=1}^{s} \epsilon_i \frac{\partial \varphi}{\partial \alpha_i}(\alpha) \right]^{[k]} \right\|_\infty \leq \sum_{\substack{i_1+\cdots+i_s=k \\ i_j \in \{0,1\}}} \frac{k!}{i_1! \cdots i_s!} |\epsilon_1|^{i_1} \cdots |\epsilon_s|^{i_s} \left\| \frac{\partial^k \varphi}{\partial \alpha_1^{i_1} \cdots \partial \alpha_s^{i_s}}(\alpha) \right\|_\infty$$

then

$$\left\| \left[\sum_{i=1}^{s} \epsilon_i \frac{\partial \varphi}{\partial \alpha_i}(\alpha) \right]^{[k]} \right\|_\infty \leq \binom{s}{k} k! \epsilon_\alpha^k \max\left(1, \max_{j=k+1,\ldots,s}\left(\binom{s-k}{j-k} M_\alpha^{j-k}\right)\right).$$

As $\epsilon_\alpha < 1$ we deduce the claim. □

Corollary 3.2: *With the previous notations, if the error ϵ_α is bounded by:*

$$(*) \quad \epsilon_\alpha \leq 0.5 \left(1 + \sum_{k=1}^{s-1} \binom{s}{k} \max\left(1, \max_{j=k+1,\ldots,s}\left(\binom{s-k}{j-k} M_\alpha^{j-k}\right)\right)\right)^{-1}$$

then the error on the coefficient of $f_{\tilde{\alpha}}$ is smaller than 0.5.

Corollary 3.3: *Let α be a coefficient of P_1 such that α has degree s over $\mathbb{Q}$. If ϵ_α satisfies*

$$\epsilon_\alpha \leq 0.5 \left(1 + \sum_{k=1}^{s-1} \binom{s}{k} \max\left(1, \max_{j=k+1,\ldots,s}\left(\binom{s-k}{j-k} \left(2^{2n} \|P\|_\infty\right)^{j-k}\right)\right)\right)^{-1}$$

then we can recognize $f_\alpha(T)$ from $f_{\tilde{\alpha}}(T)$.

Remark: We get the same kind of bound if the primitive element α is a linear combination of the coefficients of P_1. In this case, we substitute $2^{2n}\|P\|_\infty$ by $\left(\sum_{i,j} |\lambda_{i,j}|\right) 2^{2n} \|P\|_\infty$ in the previous formula.

4. A method to obtain the exact factorization

In this section, we start with a polynomial f_α of a primitive element α of $\mathbb{K}$ obtained as explain in Section 3. To find the exact expression of the coefficients of P_1, we use an adapted representation of the coefficients of P_1.

4.1. $f'_\alpha(\alpha)$ is a common denominator

We recall a classical result of algebraic number theory.

PROPOSITION 4.1: *(see [13] page 242) Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$, $\alpha \in \mathcal{O}_\mathbb{K}$ a primitive element of $\mathbb{K}$ and f_α its minimal polynomial. Then we have:*
$\mathcal{O}_\mathbb{K} \subset \dfrac{1}{f'_\alpha(\alpha)}\mathbb{Z}[\alpha]$. *This implies that every $a \in \mathcal{O}_\mathbb{K}$ can be written:*
$a = \dfrac{z_0}{f'_\alpha(\alpha)} + \dfrac{z_1}{f'_\alpha(\alpha)}\alpha + \cdots + \dfrac{z_{s-1}}{f'_\alpha(\alpha)}\alpha^{s-1}$ *with $z_i \in \mathbb{Z}$.*

Remark: This representation has several different names: Hecke representation, Kronecker representation, and rational univariate representation. The univariate rational representation is a usefull tool in polynomial system solving (see [7]): this representation is used to solve polynomial system with the help of the Chow form of the zero dimensional component of the solution.

4.2. Recognition of the coefficients of P_1

Having the denominator $f'_\alpha(\alpha)$, we only have to recognize the numerators. Let $a_1^{(u,v)}$ be a coefficient of P_1, $a_1^{(u,v)}$ belongs to $\mathcal{O}_\mathbb{K}$. So by proposition 4.1:
$a_1^{(u,v)} = \dfrac{z_0}{f'_\alpha(\alpha)} + \dfrac{z_1}{f'_\alpha(\alpha)}\alpha + \cdots + \dfrac{z_{s-1}}{f'_\alpha(\alpha)}\alpha^{s-1}$
Applying the $\mathbb{Q}$-homomorphism σ_i, we get
$a_i^{(u,v)} = \dfrac{z_0}{f'_\alpha(\sigma_i(\alpha))} + \dfrac{z_1}{f'_\alpha(\sigma_i(\alpha))}\sigma_i(\alpha) + \cdots + \dfrac{z_{s-1}}{f'_\alpha(\sigma_i(\alpha))}\sigma_i(\alpha)^{s-1}$, then

$$(\star) \quad \begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \cdots & \sigma_1(\alpha)^{s-1} \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 & \cdots & \sigma_2(\alpha)^{s-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_s(\alpha) & \sigma_s(\alpha)^2 & \cdots & \sigma_s(\alpha)^{s-1} \end{pmatrix} \begin{pmatrix} z_0 \\ z_1 \\ \vdots \\ z_{s-1} \end{pmatrix} = \begin{pmatrix} f'_\alpha(\sigma_1(\alpha))a_1^{(u,v)} \\ f'_\alpha(\sigma_2(\alpha))a_2^{(u,v)} \\ \vdots \\ f'_\alpha(\sigma_s(\alpha))a_s^{(u,v)} \end{pmatrix}$$

We remark that in practice we do not have $a_i^{(u,v)}$ but $a_i^{(u,v)} + \nu_i$ and we do not have $\sigma_i(\alpha)$ but $\sigma_i(\alpha) + \epsilon_i$. So we need to solve the Vandermonde system and take the nearest integer of each component of the solution. We will see that, with this method, we can certify our result.

4.3. Choice of the precision

If $\mathcal{M} = (m_{i,j})_{i,j=0}^{s-1}$ is a matrix of $\mathcal{M}_{s,s}(\mathbb{C})$ let $\|\mathcal{M}\|_\infty = \max_{i=0,\dots,s-1} \sum_{j=0}^{s-1} |m_{i,j}|$, and if $\vec{v}$ is a vector of $\mathbb{C}^s$ (with i-th coordinate equal to v_i) $\|\vec{v}\|_\infty = \max_{i=0,\dots,s-1} |v_i|$. With these notations we have $\|\mathcal{M}\vec{v}\|_\infty \le \|\mathcal{M}\|_\infty \|\vec{v}\|_\infty$.

Now we set:

$\alpha_i = \sigma_i(\alpha)$, ϵ_i is the error on α_i, ν_i is the error on $a_i^{(u,v)}$,
e_i is the error on z_i, ϵ is a real number such that: $\begin{cases} \forall 1 \leq i \leq s & |\epsilon_i| \leq \epsilon < 1 \\ \forall 1 \leq i \leq s & |\nu_i| \leq \epsilon < 1 \end{cases}$,
M is the real number: $\max_{i,u,v} |a_i^{(u,v)}| = M$.
Thanks to corollary 3.1 we can write $M \leq 2^{2n} \|P\|_\infty$.
We set

$$\vec{\alpha} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix}, \quad \vec{z} = \begin{pmatrix} z_0 \\ \vdots \\ z_{s-1} \end{pmatrix}, \quad \vec{a}^{(u,v)} = \begin{pmatrix} a_1 \\ \vdots \\ a_s \end{pmatrix}, \quad \vec{e} = \begin{pmatrix} e_1 \\ \vdots \\ e_s \end{pmatrix},$$

$$\vec{\epsilon_\alpha} = \begin{pmatrix} \epsilon_0 \\ \vdots \\ \epsilon_{s-1} \end{pmatrix}, \quad \vec{\nu} = \begin{pmatrix} \nu_0 \\ \vdots \\ \nu_{s-1} \end{pmatrix},$$

$$M(\alpha) = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{s-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{s-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_s & \alpha_s^2 & \cdots & \alpha_s^{s-1} \end{pmatrix}^{-1} \begin{pmatrix} f'_\alpha(\alpha_1) & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & & \\ 0 & \dots & f'_\alpha(\alpha_k) & \dots & 0 \\ \vdots & & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & f'_\alpha(\alpha_s) \end{pmatrix}.$$

Then the equality: $\vec{z} + \vec{e} = M(\vec{\alpha} + \vec{\epsilon_\alpha})(\vec{a}^{(u,v)} + \vec{\nu})$ holds.
Now, we give a sufficient condition on ϵ which allows us to certify that $\|\vec{e}\|_\infty < 0.5$. The strategy is the following: we express the coefficient of $M(\vec{\alpha})$ in function of α_i, and then deduce this inequality.

$$\|\vec{e}\|_\infty \leq (\|M(\vec{\alpha})\|_\infty + \|N\|_\infty(1 + M))\,\epsilon$$

LEMMA 4.1: *Let $M(\vec{\alpha}) = (m_{i,j}(\alpha))_{i,j=0}^{s-1}$ then we have:*

$$m_{i,j}(\alpha) = (-1)^{s-i-1} S_{s-i-1}(\alpha_1, \dots, \alpha_j, \alpha_{j+2}, \dots, \alpha_s)$$

Proof: We denote $V(\alpha)^{-1} = (w_{i,j}(\alpha))_{i,j=0}^{s-1}$ the inverse of the Vandermonde matrix.
The value of the polynomial $l_k(x) = \sum_{j=0}^{s-1} w_{j,k} x^j$ is 1 when $x = \alpha_{k+1}$ and it is 0 when $x \in \{\alpha_1, \dots, \alpha_s\} \setminus \{\alpha_{k+1}\}$. Hence $l_k(x)$ is the Lagrange's polynomial and we get:

$$l_k(x) = \prod_{\substack{i=1 \\ i \neq k+1}}^{s} \left(\frac{x - \alpha_i}{\alpha_{k+1} - \alpha_i} \right) = \prod_{\substack{i=1 \\ i \neq k+1}}^{s} (x - \alpha_i) \times \frac{1}{f'_\alpha(\alpha_{k+1})}.$$

Therefore

$$w_{j,k}(\alpha) = \frac{(-1)^{s-1-j} S_{s-j-1}(\alpha_1, \dots, \alpha_k, \alpha_{k+2}, \dots, \alpha_s)}{f'_\alpha(\alpha_{k+1})}$$

where S_k is the k^{th} elementary symmetric polynomial (see Section 3.4), and we set $S_0 = 1$.
The definition of $M(\vec{\alpha})$ gives $m_{i,j}(\alpha) = w_{i,j}(\alpha) f'_\alpha(\alpha_{j+1})$. Thus the claim is proved. □

Corollary 4.1: *There exists a matrix $N \in \mathcal{M}_{s,s}(\mathbb{C})$ such that:*

$$\|M(\vec{\alpha}+\vec{\epsilon}) - M(\vec{\alpha})\|_\infty \leq \epsilon \|N\|_\infty$$

with $\|N\|_\infty \leq s\left(1 + \sum_{k=1}^{s-2} \binom{s-1}{k} \max\big(1, \max_{j=k+1,\dots,s-1}\big(\binom{s-1-k}{j-k} M^{j-k}\big)\big)\right)$.

Proof: Apply lemma 3.3. □

Lemma 4.2: *With the previous notations*

$$\|\vec{e}\|_\infty \leq (\|M(\vec{\alpha})\|_\infty + \|N\|_\infty(1+M))\epsilon.$$

Proof: The equalities $\vec{z} + \vec{e} = M(\vec{\alpha}+\vec{\epsilon})(\vec{a}+\vec{\nu})$ and $\vec{z} = M(\vec{\alpha})\vec{a}$ give $\|\vec{e}\|_\infty \leq \epsilon\|N\|_\infty\|\vec{a}\|_\infty + \big(\|M(\vec{\alpha})\|_\infty + \epsilon\|N\|_\infty\big)\|\vec{\nu}\|_\infty$. This implies the desired result. □

The previous results of this section imply:

Proposition 4.2: *If the error ϵ is such that*

$$\begin{aligned}\epsilon \ \leq 0.5 \ & \Bigg[\max_{i=0,\dots,s-1}\Big(s\binom{s-1}{s-i-1}M^{s-i-1}\Big) \\ & +s\left(1 + \sum_{k=1}^{s-2} \binom{s-1}{k} \max\big(1, \max_{j=k+1,\dots,s-1}\big(\binom{s-1-k}{j-k} M^{j-k}\big)\big)\right)(1+M)\Bigg]^{-1},\end{aligned}$$

then we can, with the system $(\star)$, recognize the exact coefficients of P_1.

Proof: Lemma 4.1 gives: $|m_{i,j}(\alpha)| \leq S_{s-i-1}(|\alpha_1|, \dots, |\alpha_j|, |\alpha_{j+2}|, \dots, |\alpha_s|)$.
So: $|m_{i,j}(\alpha)| \leq \sum_{1\leq k_1 < .. < k_{s-i-1} \leq s-1} M^{s-i-1} \leq \binom{s-1}{s-i-1} M^{s-i-1}$. It follows

$$\sum_{j=0}^{s-1} |m_{i,j}(\alpha)| \leq \sum_{j=0}^{s-1} \binom{s-1}{s-i-1} M^{s-i-1} = s\binom{s-1}{s-i-1} M^{s-i-1}.$$

Thus: $\|M(\alpha)\|_\infty \leq \max_{i=0,\dots,s-1}\Big(s\binom{s-1}{s-i-1}M^{s-i-1}\Big)$.

Together with corollary 4.1 this implies

$$\begin{aligned}\|\vec{e}\|_\infty \ \leq \ & \Bigg[\max_{i=0,\dots,s-1}\Big(s\binom{s-1}{s-i-1}M^{s-i-1}\Big) \\ & + s\left(1 + \sum_{k=1}^{s-2} \binom{s-1}{k} \max\big(1, \max_{j=k+1,\dots,s-1}\big(\binom{s-1-k}{j-k} M^{j-k}\big)\big)\right)(1+M)\Bigg]\epsilon.\end{aligned}$$

So we get the announced bound. □

We can write proposition 4.2 with $2^{2n}\|P\|_\infty$ instead of M. In this case we have a formula depending only on $\|P\|_\infty$, s and n. As s can be bounded by n, we can write a condition which relies on the height and the degree of the polynomial P.

COROLLARY 4.2: *If the error ϵ is bounded by*

$$\epsilon \quad \leq 0.5 \quad \Bigg[\max_{i=0,\dots,n-1} (n \binom{n-1}{n-i-1} (2^{2n}\|P\|_\infty)^{n-i-1})$$
$$+n \left(1 + \sum_{k=1}^{n-2} \binom{n-1}{k} \max\big(1, \max_{j=k+1,\dots,n-1} (\binom{n-1-k}{j-k} (2^{2n}\|P\|_\infty)^{j-k})\big) \right) (1 + (2^{2n}\|P\|_\infty)) \Bigg]^{-1}$$

then we can, with the system ($\star$), recognize the exact coefficients of P_1.

4.4. Conversion

Let $\beta \in \mathcal{O}_{\mathbb{K}}$. We have the two following representations:

$\beta = \displaystyle\sum_{j=0}^{s-1} \frac{z_j}{f'_\alpha(\alpha)} \alpha^j = \sum_{i=0}^{s-1} q_i \alpha^i$ where $z_j \in \mathbb{Z}$ and $q_i \in \mathbb{Q}$.

Let $B(\alpha)$ be the inverse of $f'_\alpha(\alpha)$, and set $\alpha^j B(\alpha) = \displaystyle\sum_{i=0}^{s-1} b_{i,j}\alpha^i$ where $b_{i,j} \in \mathbb{Q}$. It can be easily computed once for all coefficients of P_1.

LEMMA 4.3: *With the previous notations and with*

$$\vec{q} = \begin{pmatrix} q_0 \\ \vdots \\ q_{s-1} \end{pmatrix}, \quad \vec{z} = \begin{pmatrix} z_0 \\ \vdots \\ z_{s-1} \end{pmatrix}, \quad \text{and} \quad \mathcal{M}_B = (b_{i,j})_{i,j=0}^{s-1} \in \mathcal{M}_{s,s}(\mathbb{Q}),$$

we have $\vec{q} = \mathcal{M}_B(\vec{z})$.

4.5. The algorithm

Input: $P \in \mathbb{Z}[X,Y]$ irreducible in $\mathbb{Q}[X,Y]$, monic in Y.

1. Compute an approximate absolute factorization of P, with a precision ϵ satisfying the inequality of proposition 4.2.
2. Recognize a primitive element of $\mathbb{K}$ and its minimal polynomial as explained in section 3. Denote by f_α its minimal polynomial.
3. Recognize the exact coefficients of P_1 by solving a Vandermonde system. Give for each coefficient of P_1 its canonical expression in $\mathbb{Q}[\alpha]$.

Output: The minimal polynomial of a primitive element of $\mathbb{K}$ and $P_1(X,Y) \in \mathbb{K}[X,Y]$ an absolute factor of P.

Remark: We do not need to check that the constructed polynomial divides P. Inded by step 1 we know that we have a sufficient precision. Thus we deduce that the error on the integer numbers is smaller than 0.5. So when we take the nearest integer we obtain the “good”integer.

4.6. A small example

Here we illustrate the different steps of the algorithm on a small example.

Input: $P(X,Y) = Y^4 + 2Y^2X + 14Y^2 - 7X^2 + 6X + 47 \in \mathbb{Z}[X,Y]$.
P is irreducible in $\mathbb{Q}[X,Y]$.

`Step` 1)
We apply an approximate absolute polynomial factorization to P (see for example [15], [20], [2]) with a precision $\epsilon := 10^{-4}$, and we get:
$\tilde{P}_1(X,Y) = Y^2 + 3.828X + 8.414$,
$\tilde{P}_2(X,Y) = Y^2 - 1.828X + 5.585$.

We have $s = 2$ and we can take $M = 10$ (in fact we have to choose $M \geq 8.414$). These values ϵ, s and M satisfy the inequality of proposition 4.2. Thus we can recognize the exact absolute irreducible factorization from the approximate one.

`Step` 2)
We note $\tilde{a}_i^{(u,v)}$ the coefficients of $\tilde{P}_i$.
$\tilde{a}_1^{(0,0)} = 8.414$, $\tilde{a}_2^{(0,0)} = 5.585$, $\tilde{a}_1^{(1,0)} = 3.828$, $\tilde{a}_2^{(1,0)} = -1.828$.
We have:
$f_{\tilde{a}_1^{(0,0)}} = (T - 8.414)(T - 5.585) = T^2 - 13.999T + 46.992$
$f_{\tilde{a}_1^{(1,0)}} = (T + 1.828)(T - 3.828) = T^2 - 2.00T - 6.997$.
Thus $f_{a_1^{(0,0)}} = T^2 - 14T + 47$, and $f_{a_1^{(1,0)}} = T^2 - 2t - 7$.

As $\gcd(f_{a_1^{(0,0)}}, f'_{a_1^{(0,0)}}) = 1$, $\alpha = a_1^{(0,0)}$ is a primitive element of $\mathbb{K}$, and $f_\alpha(T) = T^2 - 14T + 47$.

`Step` 3)
We have $f'_\alpha(\tilde{a}_1^{(0,0)}) \approx 2.828$, and $f'_\alpha(\tilde{a}_2^{(0,0)}) \approx -2.830$, this gives

$$\begin{pmatrix} 1 & 8.414 \\ 1 & 5.585 \end{pmatrix} \begin{pmatrix} \tilde{z}_0 \\ \tilde{z}_1 \end{pmatrix} = \begin{pmatrix} 2.828 \times 3.828 \\ -2.830 \times (-1.828) \end{pmatrix}$$

This gives $\tilde{z}_0 = -5.989$ and $\tilde{z}_1 = 1.998$.
So $z_0 = -6$, $z_1 = 2$ and $a_1^{(1,0)} = \dfrac{-6}{f'_\alpha(\alpha)} + 2\dfrac{\alpha}{f'_\alpha(\alpha)}$.

We have $f_\alpha(T) = T^2 - 14T + 47$, $f'_\alpha(T) = 2T - 14$ and:

$$-\frac{1}{2}f_\alpha(T) + f'_\alpha(T)(\frac{1}{4}T - \frac{7}{4}) = 1.$$

This implies: $\dfrac{1}{4}T - \dfrac{7}{4} = f'_\alpha(\alpha)^{-1}$.

Thus $a_1^{(1,0)} = \dfrac{-6}{f'_\alpha(\alpha)} + 2\dfrac{\alpha}{f'_\alpha(\alpha)} = -13 + 2\alpha$.

Outputs: $f_\alpha(T) = T^2 - 14T + 47$,
$P_1(X,Y) = Y^2 + (-13 + 2\alpha)X + \alpha$.

5. Conclusion

In this paper we applied Number Theory techniques and provided sharp bounds to greatly improve an algorithm of absolute factorization described in [15], [5]. This previous algorithm relied on the command *bestapprox* of the PARI system which uses on a continued fraction representation of the number and detects a size gap in the convergent, see [4]. Although this heuristic can give a good guess in most cases, our new approach is more rigorous, safer and more efficient. Indeed, we do not have to compute a continued fraction, we just have to take the nearest integer of a real number.
The method esposed here is one of the key ingredients of a new algorithm and its implementation described in [2], and [1]. With this symbolic-numeric implementation we can compute the exact absolute factorization of a bivariate polynomial with total degree 200 having 10 absolute irreducible factors in approximatively 15 minutes. In this case, the step "approximate to exact factorization"takes only 15 secondes of these 15 minutes. In conclusion, the method presented in this paper allows us to get in a quick and efficient way an exact absolute factorization with symbolic-numeric tools.

6. Acknowledgment

The authors would like to thanks the anonymous referees for their helpful coments.

References

1. Guillaume Chèze. *Des méthodes symboliques-numériques et exactes pour la factorisation absolue des polynômes en deux variables.* PhD thesis, Université de Nice-Sophia Antipolis, 2004.

2. Guillaume Chèze. Absolute polynomial factorization in several variables and the knapsack problem. In *Proceedings of ISSAC 2004*, pages 87–94, 2004.

3. Guillaume Chèze and André Galligo. Four lessons on absolute polynomial factorization. In I.Z.Emiris A.Dickenstein, editor, *Solving Polynomial Equations*, volume 14 of *Algorithms and Computation in Mathematics*, pages 331–383. Springer-Verlag, 2005.

4. Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

5. R.M. Corless, A. Galligo, I.S. Kotsireas, and S.M. Watt. A geometric-numeric algorithm for factoring multivariate polynomials. In T. Mora, editor, *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC 2002)*, pages 37–45. ACM, 2002.

6. David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

7. M. Elkadi and B. Mourrain. Symbolic-numeric methods for solving polynomial equations and applications. In I.Z.Emiris A.Dickenstein, editor, *Solving Polynomial Equations*, volume 14 of *Algorithms and Computation in Mathematics*, pages 331–383. Springer-Verlag, 2005.

8. André Galligo. Real factorization of multivariate polynomials with integer coefficients. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 258(Teor. Predst. Din. Sist. Komb. i Algoritm. Metody. 4):60–70, 355, 1999.

9. André Galligo and David Rupprecht. Irreducible decomposition of curves. *J. Symbolic Comput.*, 33(5):661–677, 2002. Computer algebra (London, ON, 2001).

10. Shuhong Gao, Erich Kaltofen, John P. May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials via differential equations. In *Proceedings of ISSAC 2004*, pages 167–174, 2004.

11. Erich Kaltofen and John May. On approximate irreducibility of polynomials in several variables. In *Proceedings of ISSAC 2003*, pages 161–168, 2003.

12. Maurice Mignotte and Doru Ştefănescu. *Polynomials*. Springer Series in Discrete Mathematics and Theoretical Computer Science. Springer-Verlag Singapore, Singapore, 1999.

13. Paulo Ribenboim. *Classical theory of algebraic numbers*. Universitext. Springer-Verlag, New York, 2001.

14. David Rupprecht. *Elements de géométrie algébrique approchée: Etude du pgcd et de la factorisation*. PhD thesis, Univ. Nice Sophia Antipolis, 2000.

15. David Rupprecht. Semi-numerical absolute factorization of polynomials with integer coefficients. *J. Symbolic Comput.*, 37:557–574, 2004.

16. Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967.

17. T. Sasaki. Approximate multivariate polynomial factorization based on zero-sum relations. In B. Mourrain, editor, *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (ISSAC 2001)*, pages 284–291. ACM, 2001.

18. A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.

19. J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Comput. Mach.*, 27(4):701–717, 1980.

20. Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler. Numerical factorization of multivariate complex polynomials. *Theoret. Comput. Sci.*, 315(2-3):651–669, 2004.

21. Richard Zippel. *Effective polynomial computation*. Kluwer Academic Publishers, 1993.