Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Symbolic Computation 41 (2006) 682–696
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

# From an approximate to an exact absolute polynomial factorization

Guillaume Chèze*, André Galligo

*Laboratoire de Mathématiques, Université de Nice Sophia Antipolis, Parc Valrose, Nice 06108 Cedex 2, France*

Received 19 November 2003; accepted 16 November 2005
Available online 20 January 2006

**Abstract**

We propose an algorithm for computing 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.


*Keywords:* Absolute factorization; Algebraic integers; Vandermonde matrix

## 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. Galligo (1999), Corless et al. (2002), Rupprecht (2000), Sasaki (2001), Sommese et al. (2004), Galligo and Rupprecht (2002), Chèze (2004b) and Chèze and Galligo (2005). For the study of approximate irreducibility and approximate factorization, one could see Kaltofen and May (2003) and Gao et al. (2004).

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

* Corresponding author. Tel.: +33 04 93 07 62 37; fax: +33 04 93 51 79 74.
*E-mail addresses:* cheze@math.unice.fr (G. Chèze), galligo@math.unice.fr (A. Galligo).

0747-7171/$ - see front matter 
doi:10.1016/j.jsc.2005.11.004

$\tilde{P}_i \in \mathbb{C}[X, Y]$ and the coefficients of $\tilde{P}_i$ are numerical approximations of the coefficients of $P_i$ with a given precision $\epsilon$. That is to say $\|P_i - \tilde{P}_i\|_\infty < \epsilon$ with respect to the norm $\|\sum_{i,j} a_{i,j} X^i Y^j\|_\infty = \max_{i,j} |a_{i,j}|$. When $P(X, Y) \in \mathbb{Z}[X, Y]$ the norm $\|P\|_\infty$ is called the height of $P$ (and we will see that we can restrict our study to the case $P(X, Y) \in \mathbb{Z}[X, Y]$).

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 $\alpha$ over $\mathbb{Q}$, and how can we express the coefficients of $P_1$ in $\mathbb{Q}[\alpha]$?

We will answer positively if $\epsilon$ is small enough. As the coefficients of $\tilde{P}_1$ are given with an error $\epsilon$, in order to find the minimal polynomial $f_\alpha$ of $\alpha$ ($f_\alpha \in \mathbb{Q}[T]$), we have to recognize its coefficients which are rational numbers from floating points approximations. David Rupprecht gave a preliminary study of this problem in Rupprecht (2000) and Rupprecht (2004). Here we present a complete and satisfactory answer.

### 1.1. Notation 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 $x$ 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, $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x)$ 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 vector space 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 factors $P_i$ 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 $Y$:*

$$P(X, Y) = Y^n + \sum_{k=0}^{n-1} \sum_{u+v=k} a^{(u,v)} X^u Y^v.$$

*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 as:*

$$P_i(X, Y) = Y^m + \sum_{k=0}^{m-1} \sum_{u+v=k} a_i^{(u,v)} X^u Y^v = Y^m + \sum_{k=0}^{m-1} \sum_{u+v=k} b^{(u,v)}(\alpha_i) X^u Y^v,$$

*where $b^{(u,v)} \in \mathbb{Q}[Z]$, $\deg_Z b^{(u,v)} < s$ and where $\alpha_1, \ldots, \alpha_s$ are the different conjugates over $\mathbb{Q}$ of $\alpha = \alpha_1$.*

See Rupprecht (2004, 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 $\alpha$ where $\alpha$ 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):

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

If the coefficients $a_1^{(u,v)}$ are exactly known, then to check whether $P_{char}(a_1^{(u,v)})$ is the minimal polynomial of $a_1^{(u,v)}$ over $\mathbb{Q}$, we just have to compute the gcd of $P_{char}(a_1^{(u,v)})$ and $\frac{\partial}{\partial T} P_{char}(a_1^{(u,v)})$, 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 $\epsilon$, on the errors $\epsilon_i$. 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 expressions of the coefficients of $P_1$ in $\mathbb{K}$. We rely on the fundamental lemma and an adapted representation of these algebraic integers over $\mathbb{Z}$.

## 2. A tool-bag

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

Let $Q(X,Y) = \sum_{i=0}^{n} \sum_{j=0}^{i} q_{j,n-i} X^j Y^{n-i}$ be an irreducible polynomial in $\mathbb{Q}[X,Y]$, monic in $Y$ and 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 $d^nQ(X,Y) = \sum_{i=0}^{n} \sum_{j=0}^{i} d^i q_{j,n-i} X^j (dY)^{n-i}$. Setting $Z = dY$ we define:

$$d^nQ(X,Y) = d^nQ\left(X, \frac{Z}{d}\right) = Z^n + dq_{1,n-1}XZ^{n-1} + \cdots + d^n q_{0,0} = P(X,Z).$$

Since $d^nQ(X,Y)$ is irreducible in $\mathbb{Q}[X,Y]$, $d^nQ(X, \frac{Z}{d})$ is irreducible in $\mathbb{Q}[X,Z]$ and 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 subfield of $\mathbb{C}$ 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 $\alpha$ 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 $\alpha$ 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. Samuel, 1967, 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 $i = 1, \ldots, s/k$ 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:

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

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 $\lambda_l$ 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 $\alpha$ 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

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

where $r_i(X) \in \mathcal{K}$ are algebraic integers over $\mathbb{Z}[X]$. (See e.g. Eisenbud, 1995, 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. □

## 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 whether there is a primitive element among all the coefficients of $P_1$. If this is not the case, we present a method for constructing a primitive element. (In our examples we always found a coefficient of $P_1$ which was a primitive element.)

### *3.1. Recognition*

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

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

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

*In this case $P_{char}(\beta)$ is the minimal polynomial $f_\beta$ of $\beta$ 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:

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

### *3.2. Construction*

If no coefficient of $P_1$ is primitive we can construct, in a deterministic or in a probabilistic way, a primitive element which is integer over $\mathbb{Z}$.

We denote by $\sigma_i$ $(1 \le i \le s)$ 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:

$$H(\lambda_{(0,0)}, \ldots, \lambda_{(1,m-1)}) = \prod_{i<j}\left(\sum_{0\le u+v\le m} \lambda_{(u,v)}(\sigma_i - \sigma_j)(a_1^{(u,v)})\right) \in \mathbb{C}[\lambda_{(i,j)}]$$

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

$$\sigma_i\left(\sum_{0\le u+v\le m} s_{(u,v)} a_1^{(u,v)}\right) \neq \sigma_j\left(\sum_{0\le u+v\le m} s_{(u,v)} a_1^{(u,v)}\right).$$

This means that $\sum_{0\le u+v\le m} s_{(u,v)} a_1^{(u,v)}$ is a primitive element.
The following probabilistic lemma (see Schwartz, 1980; Zippel, 1993) helps us to conclude:

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

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

*where $s_i$ are chosen in $S$ uniformly at random.*

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

**Proposition 3.1.** *Let $P$ be a polynomial in $\mathbb{Z}[X,Y]$ monic in $Y$ and irreducible in $\mathbb{Q}[X,Y]$, $P = P_1 \cdots P_s$ its irreducible factorization 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 finite subset of $\mathbb{Z}$.*

1. *We have the following estimation of probability:*

$$\mathcal{P}\left(\sum_{0\le u+v\le m} s_{(u,v)} a_1^{(u,v)} \text{ is primitive } \mid s_{(u,v)} \in S\right) \ge 1 - \frac{\binom{s}{2}}{|S|},$$

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

2. *There exists an algebraic integer, $\sum_{0\le u+v\le m} s_{(u,v)} a_1^{(u,v)}$, which is a primitive element and satisfies:*

$$|s_{(u,v)}| \le \frac{\binom{s}{2}}{2}.$$

**Proof.** We apply Lemma 3.2, and then we set $S = \{i \in \mathbb{Z} \mid -\binom{s}{2}/2 \le i \le \binom{s}{2}/2\}$. In this case the probability is strictly bigger than 0, then there exists a primitive element as claimed. □

**Remark.** This proposition gives a deterministic algorithm for finding an algebraic integer which is a primitive element: For each element obtained from a linear combinations with coefficients in $S = \{i \in \mathbb{Z} \mid -\binom{s}{2}/2 \le i \le \binom{s}{2}/2\}$, we test with Lemma 3.1 whether this element is primitive or not.

### *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 Schinzel, 2000; Mignotte and Ştefănescu, 1999).

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

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

*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 notation, we have:*

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

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

**Remark.** There exist other bounds on $\|P_i\|_\infty$, for example using formulae from Schinzel (2000) and Mignotte and Ştefănescu (1999), we get: $\|P_i\|_\infty \le 2^{2m}\|P\|_2$, where $\|\sum_{i,j} a_{i,j}X^iY^j\|_2 = \sqrt{\sum_{i,j} a_{i,j}^2}$.

**Corollary 3.2.** 1. *If $\alpha$ is a coefficient of $P_1$ then:*

$$|\alpha| \le 2^{2n}\|P\|_\infty.$$

2. *If $\alpha$ is a primitive element obtained as explained in the second part of Proposition 3.1, then*

$$|\alpha| \le \binom{m}{2}\binom{s}{2}2^{2n-1}\|P\|_\infty.$$

**Proof.** If the primitive element $\alpha$ is a linear combination of some coefficients of $P_1$: $\alpha = \sum_{u,v} s_{(u,v)}a_1^{(u,v)}$, then we have:

$$|\alpha| \le \Big(\sum_{u,v}|s_{(u,v)}|\Big)2^{2n}\|P\|_\infty \le \binom{m}{2}\binom{s}{2}2^{2n-1}\|P\|_\infty.$$

Indeed, we have seen in Proposition 3.1 that we can suppose $|s_{(u,v)}| \le \binom{s}{2}/2$. □

*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 is written as:

$$f_{\tilde{\alpha}}(T) = \prod_{k=1}^{s}(T - (\alpha_k + \epsilon_k)).$$

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:

$$\varphi: \quad \mathbb{C}^s \longrightarrow \mathbb{C}^s$$

$$\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_k\\ \vdots\\ \alpha_s\end{pmatrix} \longmapsto \begin{pmatrix} S_1(\alpha_1,\dots,\alpha_s) & = & \alpha_1+\alpha_2+\cdots+\alpha_s\\ & \vdots & \\ S_k(\alpha_1,\dots,\alpha_s) & = & \displaystyle\sum_{1\le i_1<\cdots<i_k\le s}\alpha_{i_1}\cdots\alpha_{i_k}\\ & \vdots & \\ S_s(\alpha_1,\dots,\alpha_s) & = & \alpha_1\times\cdots\times\alpha_s\end{pmatrix}.$$

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 $\epsilon$ which will imply $\|\varphi(\alpha+\epsilon)-\varphi(\alpha)\|_\infty < 0.5$. $\varphi$ is a polynomial map such that the degree of each component is smaller than or equal to $s$ and is of degree 1 in each variable. With the following notation:

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

the Taylor expansion of $\varphi$ 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 $\epsilon_\alpha$ and $M_\alpha$ such that:

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

**Remark.** Thanks to Corollary 3.2, we can set $M_\alpha := 2^{2n}\|P\|_\infty$ if $\alpha$ is a coefficient of $P_1$, and $M_\alpha := \binom{m}{2}\binom{s}{2}2^{2n-1}\|P\|_\infty$ if $\alpha$ is obtained as explained in the second part of Proposition 3.1.

Thus we can express $M_\alpha$ in terms of $\|P\|_\infty$ (the height of $P \in \mathbb{Z}[X,Y]$), its degree $n$ and the number of absolute factors $s$.

Now we give a bound on $\epsilon_\alpha$, in order to get the exact minimal polynomial from the approximate one.

**Lemma 3.3.** *With the previous notation, we have:*

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

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

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

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

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

As a result we obtain:

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

It follows that:

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

and then

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

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

**Corollary 3.3.** *With the previous notation, if the error $\epsilon_\alpha$ is bounded by:*

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

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

**Proposition 3.3.** 1. *Let $\alpha$ be a coefficient of $P_1$ such that $\alpha$ has degree $s$ over $\mathbb{Q}$. If $\epsilon_\alpha$ satisfies*

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

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

2. *Let $\alpha$ be a primitive element obtained as explained in the second part of Proposition 3.1. If $\epsilon_\alpha$ satisfies*

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

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

## 4. A method for obtaining the exact factorization

In this section, we start with a polynomial $f_\alpha$ of a primitive element $\alpha$ of $\mathbb{K}$ obtained as explained in Section 3. To find the exact expressions 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 Ribenboim, 2001, 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 $f_\alpha$ its minimal polynomial. Then we have: $\mathcal{O}_\mathbb{K} \subset \frac{1}{f'_\alpha(\alpha)}\mathbb{Z}[\alpha]$. This implies that every $a \in \mathcal{O}_\mathbb{K}$ can be written:*

$$a = \frac{z_0}{f'_\alpha(\alpha)} + \frac{z_1}{f'_\alpha(\alpha)}\alpha + \cdots + \frac{z_{s-1}}{f'_\alpha(\alpha)}\alpha^{s-1} \text{ with } z_i \in \mathbb{Z}.$$

**Remark.** This representation has several different names: Hecke representation, Kronecker representation, and rational univariate representation. The univariate rational representation is a useful tool in polynomial system solving (see Elkadi and Mourrain, 2005; Rouillier, 1999).

*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:

$$a_1^{(u,v)} = \frac{z_0}{f'_\alpha(\alpha)} + \frac{z_1}{f'_\alpha(\alpha)}\alpha + \cdots + \frac{z_{s-1}}{f'_\alpha(\alpha)}\alpha^{s-1}.$$

Applying the $\mathbb{Q}$-homomorphism $\sigma_i$, we get

$$a_i^{(u,v)} = \frac{z_0}{f'_\alpha(\sigma_i(\alpha))} + \frac{z_1}{f'_\alpha(\sigma_i(\alpha))}\sigma_i(\alpha) + \cdots + \frac{z_{s-1}}{f'_\alpha(\sigma_i(\alpha))}\sigma_i(\alpha)^{s-1},$$

then

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

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

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

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

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

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

Then the equality: $\vec{z} + \vec{e} = M(\vec{\alpha} + \vec{\epsilon_\alpha})(\vec{a}^{(u,v)} + \vec{v})$ holds.

Now, we give a sufficient condition on $\epsilon$ which allows us to certify that $\|\vec{e}\|_\infty < 0.5$. The strategy is the following: we express the coefficients of $M(\vec{\alpha})$ as functions of $\alpha_i$, and then deduce this inequality.

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

**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 by $V(\alpha)^{-1} = (w_{i,j}(\alpha))_{i,j=0}^{s-1}$ 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* $\|N\|_\infty \leq s\left(1 + \sum_{k=1}^{s-2} \binom{s-1}{k} \max\left(1, \max_{j=k+1,\dots,s-1}\left(\binom{s-1-k}{j-k} M^{j-k}\right)\right)\right)$.

**Proof.** Apply Lemma 3.3. □

**Lemma 4.2.** *With the previous notation*

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

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

The previous results of this section imply:

**Proposition 4.2.** *If the error $\epsilon$ is such that*

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

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

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

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

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

Together with Corollary 4.1 this implies

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

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 $P \in \mathbb{Z}[X, Y]$.

**Corollary 4.2.** *If the error $\epsilon$ is bounded by*

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

*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 following two representations:

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

Let $B(\alpha)$ be the inverse of $f'_\alpha(\alpha)$, and set $\alpha^j B(\alpha) = \sum_{i=0}^{s-1} b_{i,j} \alpha^i$ 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 notation and with*

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

*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 $\epsilon$ satisfying the inequalities of Proposition 4.2 and 3.3.
2. Recognize a primitive element of $\mathbb{K}$ and its minimal polynomial as explained in Section 3. Denote by $f_\alpha$ 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 $P$. Indeed by step 1 we know that we have a sufficient precision. Thus we deduce that the error on the integers is smaller than 0.5. So when we take the nearest integer we obtain the exact expression.

### 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 Rupprecht (2004), Sommese et al. (2004), Chèze (2004b)) 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 $\epsilon$, $s$ 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 denote $\tilde{a}_i^{(u,v)}$ the coefficients of $\tilde{P}_i$.

$$\tilde{a}_1^{(0,0)} = 8.414, \quad \tilde{a}_2^{(0,0)} = 5.585, \quad \tilde{a}_1^{(1,0)} = 3.828, \quad \tilde{a}_2^{(1,0)} = -1.828.$$

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

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

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

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

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

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 Rupprecht (2004) and Corless et al. (2002). This previous algorithm relied on the command *bestapprox* of the PARI system which uses a continued fraction representation of the number and detects a size gap in the convergent, see Cohen (1993). Although this heuristic could 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 to a real number.

The method exposed here is one of the key ingredients of a new algorithm and its implementation described in Chèze (2004b), and Chèze (2004a). 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 approximately 15 min. In this case, the step "approximate to exact factorization" takes only 15 s of these 15 min. In conclusion, the method presented in this paper allows to get in a quick and efficient way an exact absolute factorization with symbolic–numeric tools.

## Acknowledgments

The authors would like to thank the anonymous referees for their helpful comments.

## References

Chèze, G., 2004a. Des méthodes symboliques–numériques et exactes pour la factorisation absolue des polynômes en deux variables. Ph.D. Thesis. Université de Nice-Sophia Antipolis.

Chèze, G., 2004b. Absolute polynomial factorization in several variables and the knapsack problem. In: Proceedings of ISSAC 2004. pp. 87–94.

Chèze, G., Galligo, A., 2005. Four lessons on absolute polynomial factorization. In: Emiris, I.Z., Dickenstein, A. (Eds.), Solving Polynomial Equations. In: Algorithms and Computation in Mathematics, vol. 14. Springer-Verlag, pp. 331–383.

Cohen, H., 1993. A Course in Computational Algebraic Number Theory. In: Graduate Texts in Mathematics, vol. 138. Springer-Verlag, Berlin.
Corless, R.M., Galligo, A., Kotsireas, I.S., Watt, S.M., 2002. A geometric–numeric algorithm for factoring multivariate polynomials. In: Mora, T. (Ed.), Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation. ISSAC 2002. ACM, pp. 37–45.
Eisenbud, D., 1995. Commutative Algebra. In: Graduate Texts in Mathematics, vol. 150. Springer-Verlag, New York. With a view toward algebraic geometry.
Elkadi, M., Mourrain, B., 2005. Symbolic–numeric methods for solving polynomial equations and applications. In: Emiris, I.Z., Dickenstein, A. (Eds.), Solving Polynomial Equations. In: Algorithms and Computation in Mathematics, vol. 14. Springer-Verlag, pp. 331–383.
Galligo, A., 1999. 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.
Galligo, A., Rupprecht, D., 2002. Irreducible decomposition of curves. J. Symbolic Comput. 33 (5), 661–677. Computer algebra (London, ON, 2001).
Gao, S., Kaltofen, E., May, J.P., Yang, Z., Zhi, L., 2004. Approximate factorization of multivariate polynomials via differential equations. In: Proceedings of ISSAC 2004. pp. 167–174.
Kaltofen, E., May, J., 2003. On approximate irreducibility of polynomials in several variables. In: Proceedings of ISSAC 2003. pp. 161–168.
Mignotte, M., Ştefănescu, D., 1999. Polynomials. In: Springer Series in Discrete Mathematics and Theoretical Computer Science, Springer-Verlag, Singapore, Singapore.
Ribenboim, P., 2001. Classical Theory of Algebraic Numbers. In: Universitext., Springer-Verlag, New York.
Rouillier, F., 1999. Solving zero-dimensional systems through the rational univariate representation. J. Appl. Algebra Eng. Commun. Comput. 9 (5), 433–461.
Rupprecht, D., 2000. Elements de géométrie algébrique approchée: Etude du pgcd et de la factorisation. Ph.D. Thesis, Univ. Nice Sophia Antipolis.
Rupprecht, D., 2004. Semi-numerical absolute factorization of polynomials with integer coefficients. J. Symbolic Comput. 37, 557–574.
Samuel, P., 1967. Théorie Algébrique Des Nombres. Hermann, Paris.
Sasaki, T., 2001. Approximate multivariate polynomial factorization based on zero-sum relations. In: Mourrain, B. (Ed.), Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation. ISSAC 2001. ACM, pp. 284–291.
Schinzel, A., 2000. Polynomials with Special Regard to Reducibility. In: Encyclopedia of Mathematics and its Applications, vol. 77. Cambridge University Press, Cambridge (With an appendix by Umberto Zannier).
Schwartz, J.T., 1980. Fast probabilistic algorithms for verification of polynomial identities. J. Assoc. Comput. Mach. 27 (4), 701–717.
Sommese, A.J., Verschelde, J., Wampler, C.W., 2004. Numerical factorization of multivariate complex polynomials. Theoret. Comput. Sci. 315 (2–3), 651–669.
Zippel, R., 1993. Effective Polynomial Computation. Kluwer Academic Publishers.