Absolute polynomial factorization in two variables and the knapsack problem

Guillaume Cheze
Laboratoire de mathématiques J.A. Dieudonné,
Université de Nice Sophia Antipolis,
Parc Valrose, Nice 06108 Cedex 2 France
cheze@math.unice.fr

Keywords
Absolute Factorization, LLL algorithm, knapsack problem

ABSTRACT
A recent algorithmic procedure for computing the absolute factorization of a polynomial $P(X,Y)$, after a linear change of coordinates, is via a factorization modulo X^3. This was proposed by A. Galligo and D. Rupprecht in [16], [8]. Then absolute factorization is reduced to finding the minimal zero sum relations between a set of approximated numbers b_i, $i=1$ to n such that $\sum_{i=1}^{n} b_i = 0$, (see also [17]). Here this problem with an a priori exponential complexity, is efficiently solved for large degrees ($n > 100$). We rely on L.L.L. algorithm, used with a strategy of computation inspired by van Hoeij's treatment in [23]. For that purpose we prove a theorem on bounded integer relations between the numbers b_i, also called linear traces in [19]

1. INTRODUCTION
Thanks to Bertini's theorem and Hensel liftings, multivariate factorization can be reduced to bivariate factorization (see e.g. [9], [13], [24]). For a polynomial $P(X,Y) \in \mathbb{Q}[X,Y]$ irreducible in $\mathbb{Q}[X,Y]$ and monic in Y, an important algorithmic question is to compute the absolute factorization of P (i.e. in $\mathbb{C}[X,Y]$). A key fact is the following:

LEMMA 1.1. *Let $P \in \mathbb{Q}[X,Y]$ be a monic and irreducible polynomial in $\mathbb{Q}[X,Y]$. $P(X,Y) = Y^n + a_{n-1}(X)Y^{n-1} + ... + a_0(X)$ with $deg(a_i(X)) \leq n-i$.*
Let $P = P_1...P_s$ 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:
$P_i(X,Y) = Y^m + b_{m-1}(\alpha_i, X)Y^{m-1} + ... + b_0(\alpha_i, X)$, with $b_k \in \mathbb{Q}[Z,X]$, $deg_X(b_k) \leq m-k$, and where $\alpha_1, ..., \alpha_s$ are the different conjugates over $\mathbb{Q}$ of $\alpha = \alpha_1$.

REMARK 1.2. *It suffices to get P_1 to describe the absolute factorization of P and obviously all factors P_i have the same degree.*

Absolute factors of a polynomial with rational coefficients have coefficients which are algebraic numbers. These can be represented either by elements in a precisely described extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$ or in $\mathbb{C}$ by imprecise floating point numbers which approximate them. This distinction gives rise to two families of algorithms: one kind of algorithm which ultimately rely on linear algebra and can be developed on $\overline{\mathbb{Q}}$, e.g. algorithms of Trager-Traverso (see [21], [22]), Kaltofen (see [11], [12]), Duval [5], Gao [9], Cormier-Singer-Trager-Ulmer [4]. Another kind of algorithms use topological properties of $\mathbb{C}^2$, Newton approximation or so called homotopy methods and for which floating point approximations are better suited, e.g. algorithms of Sasaki and coworkers (see [15], [17], [18]), Galligo and coworkers (see [3], [7], [8]), Sommese-Verschelde-Wampler (see [19], [20]). Here we follow a symbolic-numeric method to get an absolute factorization. In a first step we work with floating point number and we get an "approximate factorization modulo X^3", then we recognize the exact factors modulo X^3 (see [1]). In a second step we perform an Hensel lifting in an extension field. The aim of this paper is to present an efficient method for the first step: get an absolute factorization modulo X^3.

Let us recall the idea of Galligo-Rupprecht's algorithm (see [16]), and introduce the needed notations.
For $x_0 \in \mathbb{C}$, we denote by $y_1(x_0), \ldots, y_n(x_0)$ the roots of $P(x_0, Y)$. Then for all values of x_0 except at most $n(n-1)$, these roots are distinct and the curve defined by P is smooth nearby the points $(x_0, y_i(x_0))$, for $i = 1, \ldots, n$. If we choose such a value for x_0, then there exists analytical functions $\varphi_i(X)$ in the neighborhood of x_0 (for $i = 1, \ldots, n$) such that

$$\begin{cases} \varphi_i(x_0) = y_i(x_0) \\ P(X, \varphi_i(X)) = 0. \end{cases}$$

There exists complex number a_i and b_i (for $i = 1, \ldots, n$) such that $\varphi_i(X) = y_i(x_0) + a_i(X - x_0) + b_i(X - x_0)^2 + \ldots$.
Set $\alpha(x,y) = \frac{\partial P}{\partial x}(x,y)$, $\beta(x,y) = \frac{\partial P}{\partial y}(x,y)$, $\gamma(x,y) = \frac{\partial^2 P}{\partial x^2}(x,y)$, $\delta(x,y) = \frac{\partial^2 P}{\partial y^2}(x,y)$, $\varepsilon(x,y) = \frac{\partial^2 P}{\partial x \partial y}(x,y)$, then we have
$a_i(x_0) = -\dfrac{\alpha(x_0, y_i(x_0))}{\beta(x_0, y_i(x_0))}$, and

$$b_i(x_0) = -\frac{1}{2\beta(x_0,y_i(x_0))}\left(\gamma(x_0,y_i(x_0))+2\varepsilon(x_0,y_i(x_0))a_i(x_0)\right.$$
$$\left.+\delta(x_0,y_i(x_0))a_i^2(x_0)\right).$$

We set: $a(X,Y)=-\frac{\alpha(X,Y)}{\beta(X,Y)}$,

$$b(X,Y) = -\frac{1}{2\beta(X,Y)}\left(\gamma(X,Y)+2\varepsilon(X,Y)a(X,Y)\right.$$
$$\left.+\delta(X,Y)a(X,Y)\right)\in\mathbb{C}(X,Y).$$

Let U be a open neighborhood of x_0 in $\mathbb{C}$ where all the $\varphi_i(X)$ are defined for $i=1,\ldots,n$. As $P(X,\varphi_i(X))=0$ on U for all i, and P is monic in Y, we can write:
$P(X,Y)=\prod_{i=1}^{n}(Y-\varphi_i(X))$.
Then each factor P_k for each $k=1,\ldots,s$, of the factorization $P(X,Y)=\prod_{k=1}^{s}P_k$, writes:
$P_k(X,Y)=\prod_{j=i_1}^{i_m}(Y-\varphi_j(X))$. (1)
The total degree of P_k is m so we can write:
$P_k(X,Y)=Y^m+(q_1(X))Y^{m-1}+q_2(X)Y^{m-2}+\cdots+q_m(X)$, (2)
where $q_j(X)\in\mathbb{Q}[X]$ and $deg(q_j(X))\leq j$.
In particular, $deg(q_1(X))\leq 1$ so the coefficient of its degree two term is zero. From (1) and (2), we get $\sum_{j=i_1}^{i_m}\varphi_j(X)=q_1(X)$, thus $\sum_{j=i_1}^{i_m}b_j(X)=0$. So we found a necessary condition attached to each factor P_k of P. In fact this condition is, with a genericity hypothesis, sufficient as stated in the:

THEOREM 1.3 (GALLIGO-RUPPRECHT'S THEOREM). *Let P be an irreducible polynomial in $\mathbb{Q}[X,Y]$, monic in Y of total degree n. Consider $Q(x,y,\lambda)=P(x+\lambda y,y)$. Then for almost all specializations (x_0,λ_0) of (x,λ), the sums $\sum_{i\in J}b_i(x_0)$, for J in $\{1,\cdots,n\}$, vanish if and only if $\prod_{j\in J}(Y-\varphi_j(X))$ is a polynomial factor of P.*

This theorem gives rise to an algorithm modulo the following combinatorial problem. Given a set of complex numbers b_1, ..., b_n such that $\sum_{i=}^{n}b_i=0$, find all zero sums between these numbers. The minimal sums (i.e. with the minimal number of b_i) will correspond to the irreducible factors of P. This combinatorial problem could be solved by an extensive search among all the 2^n sums. For $n=60$, we would have to compute more than 10^{18} sums. D. Rupprecht [16] proposed several improvements for detecting vanishing sums, and drop the complexity for this step to $O(2^{n/4})$. With nowadays computers, this is easily tractable for $n=80$ but hardly tractable for $n\geq 100$.
From each minimal sum $\sum_{i\in I_k}b_i(x_0)=0$, one get the irreducible factor P_k modulo $(X-x_0)^3$, $P_k=\prod_{i\in I_k}(Y-\varphi_i(X))=\prod_{i\in I_k}(Y-(y_i+a_i(X-x_0)+b_i(X-x_0)^2))$ mod $(X-x_0)^3$. Then one obtains the absolute factorization after an Hensel lifting of $P=P_1\ldots P_s \mod (X-x_0)^3$. This provides a very efficient algorithm for medium degrees (see [16]).

Our aim is to get rid of this limitation (i.e. $n\leq 80$). We propose a new algorithm based on the L.L.L. algorithm to compute efficiently (with a polynomial complexity) the minimal sums between the b_i. In section 2 we give a more precise statement of theorem 1.3 and we recall some classical results about the L.L.L. algorithm. We prove with generic hypotheses that the only integer relation between the b_i have the following form: $\sum_{i\in I}cb_i=0$ where $\prod_{i\in I}(Y-\varphi_i(X))\in\mathbb{C}[X,Y]$ and divides $P(X,Y)$. In section 3 we will use the L.L.L. algorithm in order to find an integer relation between the $\Re(b_i)$ (the real part of b_i). Section 4 describes our algorithm and the proof that it terminates. Finally section 5 lists possible improvements of our algorithm, and some heuristics.

2. INTEGER RELATIONS BETWEEN THE NUMBERS B_I, AND L.L.L. ALGORITHM

Here we improve theorem 1.3, and recall some classical results about the L.L.L. algorithm.

2.1 A key theorem

THEOREM 2.1. *Let M be a positive constant. Let P be an irreducible polynomial in $\mathbb{Q}[X,Y]$ of total degree n, and monic in Y. Consider $Q(X,Y,\lambda)=P(X+\lambda Y,Y)$. Then for almost all specializations (x_0,λ_0) of (X,λ) the only "$M-$bounded" integer relations between the $b_i(x_0)$, (i.e. $\sum_{i\in I}\lambda_i b_i(x_0)=0$, $\lambda_i\in\mathbb{Z}$ and $|\lambda_i|\leq M$) are of the following form: $\sum_{i\in I}cb_i(x_0)=0$, where $c\in\mathbb{Z}$, and $c\neq 0$, and $\prod_{i\in I}(Y-\varphi_i(X))$ is a polynomial factor of P.*

The following theorem (see [3], [16], [19]) is the main ingredient for the proof of theorems 1.3, and 2.1:

THEOREM 2.2. *Let P be an irreducible polynomial in $\mathbb{Q}[X,Y]$, monic in Y which admits an absolute factorization $P=P_1\ldots P_s$, with $\deg(P_i)=m$. We consider the plane curve $\mathcal{C}$ in $\mathbb{C}^2$ defined by P and its s irreducible components $\mathcal{C}_i$, that we project on the $x-$axis after a generic change of coordinates. Then the first homotopy group of the complement of the discriminant locus, $\pi_1(\mathbb{C}-\Delta)$, acts on a smooth fiber as the product (with s factors) of the symmetry groups $\mathfrak{S}_m\times\ldots\times\mathfrak{S}_m$.*

We call a nontrivial relation, a relation which is not of the following form: $\sum_{i\in I}cb_i(x_0)=0$ where $c\in\mathbb{Z}$, $c\neq 0$ and $\prod_{i\in I}(Y-\varphi_i(X))$ is a polynomial factor of P.

PROOF THEOREM 2.1. First we choose a good λ_0 (i.e. such that we can apply theorem 2.2). In fact we just have to avoid a finite number of points. We can sort the $\varphi(X)$ such that the factor $P_k=\prod_{i\in\{m(k-1)+1,\ldots,mk\}}(Y-\varphi_i(X))$. For each $M-$bounded relation $\lambda_1b_1+\ldots+\lambda_nb_n$ (there are a finite number of $M-$bounded relations) which is a nontrivial relation, we mimic the proof given in [16]. We consider the product:

$$\mathcal{B}(x_0) = \prod_{(\sigma_1,\ldots,\sigma_s)\in\mathfrak{S}_m^s}\left[\sum_{i=1}^{m}\lambda_i b(x_0,\sigma_1(y_i(x_0)))+\ldots\right.$$
$$\left.+\ldots+\sum_{i=n-m+1}^{n}\lambda_i b(x_0,\sigma_s(y_i(x_0)))\right]$$

$\mathcal{B}(x_0)$ is a symmetric function in each m-tuple arguments $(y_1(x_0),\ldots,y_m(x_0))$, $(y_{m+1}(x_0),\ldots,y_{2m}(x_0))$, ..., and in $(y_{n-m+1}(x_0),\ldots,y_n(x_0))$, thus $\mathcal{B}(x_0)\in\mathbb{C}(x_0)$. As in [2] with theorem 2.2, we can show, using a path following argument and applying analytic continuation theorem, that

$\mathcal{B}(x_0) \neq 0$. Then for almost all x_0, $\lambda_1 b_1(x_0)+\ldots+\lambda_n b_{i_n}(x_0) \neq 0$ and a nontrivial relation is not satisfied for a generic x_0. $\square$

2.2 L.L.L. reduced basis

We recall some definitions and classical properties of the L.L.L. algorithm [14]. We denote by $< ., . >$ the usual scalar product of $\mathbb{R}^n$, and $\|.\|$ is the associated norm.

DEFINITION 2.3. *Let $v_1, \ldots, v_k$, k linearly independent vectors of $\mathbb{R}^n$ ($n \geq k$). We denote by v_i^* ($1 \leq i \leq k$) the orthogonal vectors obtained by the Gram-Schmidt orthogonalization process. Let $v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{i,j} v_j^*$. A basis $v_1, \ldots, v_k$ of a lattice $\mathcal{L}$ is L.L.L. reduced if and only if: $|\mu_{i,j}| \leq \frac{1}{2}$, for $1 \leq j < i \leq n$, and, $\|v_i^* + \mu_{i,i-1} v_{i-1}^*\|^2 > \frac{3}{4}\|v_{i-1}^*\|^2$ for $1 < i \leq n$.*

From a basis of a lattice $\mathcal{L}$, the L.L.L. algorithm constructs a L.L.L. reduced basis of $\mathcal{L}$.

DEFINITION 2.4. *The determinant of the lattice $\mathcal{L} \subset \mathbb{R}^n$ with basis $v_1, \ldots, v_k$ is:* $\det(\mathcal{L}) = \sqrt{\det(< v_i, v_j >)} = \prod_{i=1}^k \|v_i^*\|$.

PROPOSITION 2.5. *Let $v_1, \ldots, v_k$ be a L.L.L. reduced basis of a lattice $\mathcal{L}$.*
If for all $k \geq k_0$, $\|v_k^*\| > M$ then $\{x \in \mathcal{L} / \|x\| \leq M\} \subset Span(v_1, \ldots, v_{k_0-1}) = \{\sum_{i=1}^{k_0-1} \lambda_i v_i / \lambda_i \in \mathbb{Z}\}$.

PROPOSITION 2.6. *Let $v_1, \ldots, v_k$ be a L.L.L. reduced basis of a lattice $\mathcal{L}$. Then: $\|v_h^*\|^2 \leq 2^i \|v_{h+i}\|^2$, $h \leq i \leq k-h$.*

3. ZERO SUMS WITH L.L.L.

3.1 First remarks

♦ In all this paper we choose x_0 real. Indeed when x_0 is real then we know that if b is one of the b_i then $\overline{b}$ ($\overline{b}$ is the conjugate of b) is also one of the b_i.

♦ Our strategy is to find first all zero sums between the $\Re(b_i)$, and in a second time to deduce all zero sums between the b_i. We introduce the following notations. $\{1, \ldots, n\} = \sqcup_{i=1}^s I_i$ is the partition corresponding to the minimal sums. $I_i^{\mathbb{R}} = \{j \in I_i / b_j \in \mathbb{R}\}$, $I_i^{\mathbb{C}+} = \{j \in I_i / \Im(b_j) > 0\}$, $I_i^{\mathbb{C}-} = \{j \in I_i / \Im(b_j) < 0\}$, where $\Im(b_j)$ is the imaginary part of b_j. Now we remark that $\sum_{I_k} b_j = 0$, implies $\sum_{I_k} \overline{b_j} = 0$. Thus $\sum_{I_k} \overline{b_j} = \sum_{I_{k'}} b_j$ where $I_{k'} = \{i \in \{1, \ldots, n\} / b_i = \overline{b_j} \text{ where } j \in I_k\}$. As we have a partition either $I_k = I_{k'}$ or $I_k \cap I_{k'} = \emptyset$.
If $I_k = I_{k'}$ then $\sum_{I_k} b_j = \sum_{I_k^{\mathbb{R}}} b_j + \sum_{I_k^{\mathbb{C}+}} 2\Re(b_j)$.
If $I_k \cap I_{k'} = \emptyset$ then b_j (for all j in I_k) are not real and $\sum_{I_k} b_j + \sum_{I_{k'}} b_j = \sum_{I_k \sqcup I_{k'}} b_j = \sum_{I_k^{\mathbb{C}+} \sqcup I_{k'}^{\mathbb{C}+}} 2\Re(b_j) = 0$.
Hence if we have a zero sum among the b_i we have a zero sum among the $\Re(b_i)$. This "trick" allows us to search, in a first step, zero sums between $\frac{n+l}{2}$ real numbers, where l is the number of b_i which belongs to $\mathbb{R}$. This number l is, in general (see section 5), small compared to n ($l << n$).

♦ We recall that, in practice, we only have an approximation $\tilde{y}_i$ of y_i, thus we can only compute $\tilde{b}_i = b_i + \eta_i$. We denote by η the maximum of $|\eta_i|$, i.e. $\eta = \max_{i=1\ldots n} |\eta_i|$. Then $|\tilde{b}_i - b_i| < \eta$.
We denote by $\lfloor x \rceil$ the nearest integer to the real number x. Then for $C \in \mathbb{Z}$: $|\lfloor C\Re(\tilde{b}_i) \rceil - C\Re(b_i)| \leq \frac{1}{2} + C\eta$.

3.2 Real zero sums

In this section we explain how to get the minimal zero sums between the $\Re(b_i)$.

3.2.1 Some notations

We sort the numbers b_i in the following way: the first ones $b_1, \ldots, b_l$ belongs to $\mathbb{R}$, then $b_{l+1}, \ldots, b_{\frac{l+n}{2}}$ are such that $\Im(b_i) > 0$, and $b_{\frac{l+n}{2}+1}, \ldots, b_n$ are such that $\Im(b_i) < 0$ with the property $b_{\frac{n+l}{2}+i} = \overline{b_{l+i}}$ ($1 \leq i \leq \frac{n+l}{2} - l$). Now we consider $\Re(b_1), \ldots, \Re(b_l)$, $2\Re(b_{l+1}), \ldots, 2\Re(b_{\frac{l+n}{2}})$, and we denote by $\epsilon_i \Re(b_i)$ ($1 \leq i \leq \frac{n+l}{2}$) the real numbers satisfying $\epsilon_i \Re(b_i) = \Re(b_i)$ if $1 \leq i \leq l$, and $\epsilon_i \Re(b_i) = 2\Re(b_i)$ if $l+1 \leq i \leq \frac{n+l}{2}$.

A minimal sum between the $\epsilon_i \Re(b_i)$ is a sum $\sum_{i \in I} \epsilon_i \Re(b_i)$ where $\sum_{i \in J \subsetneq I} \epsilon_i \Re(b_i) \neq 0$.
Such a minimal zero sum between the $\epsilon_i \Re(b_i)$ is of this form: $\sum_{i=1}^{\frac{n+l}{2}} x_i \epsilon_i \Re(b_i)$ where x_i is equal to 0 or 1. We denote by $\overrightarrow{\epsilon \Re(b)}$ the vector of $\mathbb{R}^{\frac{n+l}{2}}$ whose i^{th} coordinate equals $\epsilon_i \Re(b_i)$. Then a zero sum corresponds to a 0-1 vector $v_i \in \mathbb{Z}^{\frac{n+l}{2}}$ such that $< v_i, \overrightarrow{\epsilon \Re(b)} >= 0$. We denote by V the lattice of $\mathbb{Z}^{\frac{n+l}{2}}$ generated by the linearly independent 0-1 vectors $v_1, \ldots, v_t$ corresponding to the minimal sums between the $\epsilon_i \Re(b_i)$.

3.2.2 The strategy

We want to compute the basis $v_1, \ldots, v_t$ of V. We follow the strategy developed in [23]: we construct a sequence of lattices $\mathcal{L}_i$ which eventually converges to V, and such that: $V \subset \mathcal{L}_{i+1} \subset \mathcal{L}_i \subset \mathbb{Z}^{\frac{n+l}{2}}$. We start with $\mathcal{L} = \mathbb{Z}^{\frac{n+l}{2}}$. $\mathcal{L}_{i+1}$ is deduced from $\mathcal{L}_i$ by application of the induction step explained hereafter.
Let $\mathcal{L}$ be a lattice generated by $w_1, \ldots, w_k$ where $w_i \in \mathbb{Z}^{\frac{n+l}{2}}$, such that $V \subset \mathcal{L}$. Let $p_{\mathcal{L}}$ be the following isomorphism of $\mathbb{Z}$ module.

$$\begin{array}{ccc} p_{\mathcal{L}} : \mathcal{L} & \longrightarrow & \mathcal{L}' \\ w_i = (w_{i,1}, \ldots, w_{i,\frac{n+l}{2}}) & \mapsto & (w_{i,1}, \ldots, w_{i,\frac{n+l}{2}}, \\ & & < w_i, \overrightarrow{\lfloor C\epsilon\Re(\tilde{b}) \rceil} >) \end{array}$$

where $\overrightarrow{\lfloor C\epsilon\Re(\tilde{b}) \rceil}$ is the vector whose i^{th} coordinate is equal to $\lfloor C\epsilon_i \Re(\tilde{b}_i) \rceil$.

LEMMA 3.1. *Let $\mathcal{L}$ be a lattice containing V. Set $\mathcal{L}' = p_{\mathcal{L}}(\mathcal{L})$. Let $\nu_1, \ldots, \nu_k$ be a L.L.L. reduced basis of $\mathcal{L}'$ and k_0 an integer such that: for all $i > k_0$, $\|\nu_i^*\| > M$ where $M = \sqrt{\frac{n+l}{2} + [(\frac{1}{2} + C\eta).\frac{n+l}{2}]^2}$. Then the lattice generated by $p_{\mathcal{L}}^{-1}(\nu_1), \ldots, p_{\mathcal{L}}^{-1}(\nu_{k_0})$ contains V.*

PROOF. We know that the 0-1 generators v_i of V admit less than $\frac{n+l}{2}$ coordinates equal to 1, and that $| < v_i, \overrightarrow{\lfloor C\epsilon\Re(\tilde{b}) \rceil} > | \leq (\frac{1}{2} + C\eta).\frac{n+l}{2}$. Thus $\|p_{\mathcal{L}}(v_i)\| \leq M$. Consequently:

$\{p_{\mathcal{L}}(v_1), \ldots, p_{\mathcal{L}}(v_t)\} \subset \{x \in \mathcal{L} / \|x\| \leq M\}$. Then proposition 2.5 implies: $\{p_{\mathcal{L}}(v_1), \ldots, p_{\mathcal{L}}(v_t)\} \subset Span(\nu_1, \ldots, \nu_{k_0})$. Taking the inverse images by $p_{\mathcal{L}}$, we obtain the desired result. □

The following lemma gives a necessary condition on $\mathcal{L}$ to stop the computation of our sequence. It is very close to lemma 2.8 in [23]. We need some notations: if $\mathcal{L}$ is a lattice then $\mathcal{B}_{\mathcal{L}}$ is a basis of $\mathcal{L}$. The matrix whose rows are the elements of $\mathcal{B}_{\mathcal{L}}$ is denoted by $(\mathcal{B}_{\mathcal{L}})$, and the reduced row echelon form of this matrix is denoted by $RREF(\mathcal{B}_{\mathcal{L}})$.

LEMMA 3.2. *Let $\mathcal{L}$ be a lattice which contains V. If $\mathcal{L} = V$, then each column of $RREF(\mathcal{B}_{\mathcal{L}})$ contains precisely one 1, and all other entries are 0.*

PROOF. We consider the 0-1 vectors $v_1, \ldots, v_t$ defining V, they form the basis $\mathcal{B}_V = \{v_1, \ldots, v_t\}$. This basis is already in a reduced row echelon form and each column of $(\mathcal{B}_V)$ contains precisely one 1 and all other entries are 0 (because we consider minimal sums and they come from the partition $\{1, \ldots, n\} = \sqcup_{i=1}^{s} I_i$). The unicity of the reduced row echelon form proves the lemma. □

3.3 From real zero sums to complex zero sums

We suppose that we have found the lattice V. We aim to find the lattice W generated by the 0-1 vectors $r_1, \ldots, r_s$ corresponding to the minimal sums between the complex numbers b_i, $i = 1, \ldots, s$.
We consider the map:

$$\begin{array}{rccc} f: & \mathbb{Z}^{\frac{n+l}{2}} & \longrightarrow & \mathbb{Z}^n \\ & (x_1, \ldots, x_{\frac{n+l}{2}}) & \mapsto & (x_1, \ldots, x_{\frac{n+l}{2}}, x_l, \ldots, x_{\frac{n+l}{2}}) \end{array}$$

For each 0-1 generator v_i of V we have $< v_i, \overrightarrow{\epsilon\Re(b)} >= 0$. Thus $< f(v_i), \overrightarrow{b} >= 0$, where $\overrightarrow{b}$ is the 0-1 vector of $\mathbb{C}^n$ whose i^{th} coordinate is equal to b_i.

LEMMA 3.3. *Let v be a 0-1 generator of V, i.e. it corresponds to a minimal sum between the $\epsilon_i \Re(b_i)$. If there exists an index $1 \leq j_0 \leq l$ such that $v_{j_0} \neq 0$, then $f(v)$ corresponds to a minimal sum between the b_i.*

PROOF. Obviously $f(v)$ is a 0-1 vector corresponding to a zero sum between the b_i. We just have to show that this sum is minimal. If $f(v)$ is not minimal then $f(v) = u_1 + u_2$ where u_i are 0-1 vectors. u_1 corresponds to a minimal zero sum between the b_i and $u_{1_{j_0}} \neq 0$. We have $< u_1, \overrightarrow{b} >= \sum_{i \in I_1} b_i = 0$ thus $\sum_{i \in I_1} \overline{b_i} = \sum_{i \in I_2} b_i = 0$.
We recall that the indices of all the minimal sums form a partition of $\{1, \ldots, n\}$, so either $I_1 = I_2$ or $I_1 \cap I_2 = \emptyset$. But $b_{j_0} \in I_1$ and b_{j_0} belongs to $\mathbb{R}$, then $I_1 = I_2$. Thus $u_{1_{l+j}} = u_{1_{\frac{n+l}{2}+j}}$ $(1 \leq j \leq \frac{n+l}{2} - l)$, and there exists some a in V such that $f(a) = u_1$. Now we consider $u_2 = f(v) - u_1$ and we get $u_{2_{l+j}} = u_{2_{\frac{n+l}{2}+j}}$ $(1 \leq j \leq \frac{n+l}{2} - l)$, so there exists some b in V such that $f(b) = u_2$. Hence $f(v) = f(a) + f(b) = f(a+b)$, and $v = a + b$. This contradicts the minimality of v. □

LEMMA 3.4. *Let v be a 0-1 generator of V, i.e. it corresponds to a minimal sum between the $\epsilon_i \Re(b_i)$. If $v_j = 0$ (for all $1 \leq j \leq l$), then either $f(v)$ corresponds to a minimal sum or $f(v) = u_1 + u_2$ where $u_{1_j} = u_{2_j} = 0$ for $1 \leq j \leq l$, $u_{1_{l+j}} = u_{2_{\frac{n+l}{2}+j}}$ for $1 \leq j \leq \frac{n+l}{2} - l$, $u_{1_{\frac{n+l}{2}+j}} = u_{2_{l+j}}$ for $1 \leq j \leq \frac{n+l}{2} - l$, and u_i corresponds to a minimal sum between the b_i.*

PROOF. First we set a notation: if E is a set then $|E|$ is the cardinal of this set.
It is obvious that $f(v)$ corresponds to a zero sum between the b_i. We have $< f(v), \overrightarrow{b} >= \sum_{j \in I} b_j + \sum_{j \in J} b_j = \sum_{j \in I} b_j + \overline{b_j} = \sum_{j \in I} 2\Re(b_j) =< v, \overrightarrow{\epsilon\Re(b)} >= 0$ where $I \subset \{l+1, \ldots, \frac{n+l}{2}\}$, $J = \{j / \overline{b_j} = b_i \text{ where } i \in I\}$, and $|I| = |J| = \|v\|$. Now we suppose that there exists a minimal zero sum between the b_j where j belongs to $I \sqcup J$. Then there exists a subset $H_1 \subset I \sqcup J$ such that $\sum_{j \in H_1} b_j = 0$. As $\sum_{j \in H_1} \overline{b}_j = \sum_{j \in H_2} b_j = 0$ and that the indices of the minimal sums give a partition of $\{1, \ldots, n\}$, we have $H_1 = H_2$ or $H_1 \cap H_2 = \emptyset$.
Now we consider $H_1 \cup H_2 = H$, and we have $\{\Re(b_i) / i \in H \cap I\} = \{\Re(b_i) / i \in H \cap J\}$. Then $\sum_{j \in H} b_j = 0$ implies:
$\sum_{j \in H} \Re(b_j) = \sum_{j \in H \cap I} \Re(b_j) + \sum_{j \in H \cap J} \Re(b_j)$
$= \sum_{j \in H \cap I} 2\Re(b_j) = 0$.
Thus $|H \cap I| \geq \|v\|$ because v corresponds to a minimal zero sum between the $2\Re(b_j)$ where $j \in I$. As $H \cap I \subset I$ we get $|H \cap I| \leq |I| = \|v\|$, hence $|H \cap I| = \|v\|$. With the same kinds of arguments we get $|H \cap J| = \|v\|$. Hence $|H| = 2\|v\|$. If $H_1 = H$ (i.e. $H_1 = H_2$) then $|H_1| = 2\|v\|$, and $H_1 = I \sqcup J$. In this case, we conclude that $f(v)$ corresponds to a minimal zero sum, and this proves the first part of the lemma.
If $H = H_1 \sqcup H_2$ (i.e. $H_1 \cap H_2 = \emptyset$) then $|H_1| = |H_2| = \|v\|$. In this case we have $I \sqcup J = H_1 \sqcup H_2$ and $\sum_{j \in H_j} b_j = 0$ are two minimal zero sums. These results with the definition of H_2 prove the second part of the lemma. □

With the previous lemmas we are now able to detect minimal zero sums between the b_i.

3.4 Complex zero sums

3.4.1 *One b_i belongs to $\mathbb{R}$*

We suppose that b_{i_0} belongs to $\mathbb{R}$. Let v_1 be the 0-1 vector corresponding to the minimal zero sums between the $\epsilon_j \Re(b_j)$ where b_{i_0} appears. By lemma 3.3 the factor $f(v_1)$ corresponds to the minimal sum between the b_j. Thus $\|f(v_1)\|^2 = m$ is the degree of one absolute factor. Now we consider a vector v_2 which corresponds to a minimal zero sum between the $\epsilon_j \Re(b_j)$, but here $v_{2_k} = 0$ $(1 \leq k \leq l)$. This means that in this zero sum there are no real b_j. By lemma 3.4 we know that $f(v_2)$ corresponds to a zero sum between the b_j. If $\|f(v_2)\|^2 = m$ then $f(v_2)$ corresponds to a minimal zero sum, else $\|f(v_2)\|^2 = \|u_1 + u_2\|^2 = \|u_1\|^2 + \|u_2\|^2 = 2m$ and in this case we have to compute u_1 and u_2 (see lemmas 3.5 and 3.6 below).

3.4.2 *Every b_i belongs to $\mathbb{C} - \mathbb{R}$*

Here there are two possibilities either all $f(v_i)$ have the same norm, or there are two vectors v_1 and v_2 in V such that $\|f(v_1)\| < \|f(v_2)\|$. By lemma 3.4 we know that $\|f(v)\|^2 = m$ or $2m$ for every 0-1 generator of V. Thus in the first

case, $\|f(v_1)\|^2 = \ldots = \|f(v_t)\|^2 = l$, and $l = m$ or $l = 2m$. We recall that t is the dimension of V. Furthermore if $l = m$ then $t.l = n$, else $t.l \neq n$. Hence we compute $t.l$, if $t.l = n$ then $f(v_i)$ corresponds to a minimal zero sum, else every $f(v_i) = u_{i_1} + u_{i_2}$ where u_{i_1} and u_{i_2} correspond to two minimal zero sums between the b_i. In the second case $\|f(v_1)\|^2 = m$, and $f(v_1)$ corresponds to a minimal zero sum. Hence if $f(v)$ is such that $\|f(v)\| = \|f(v_1)\|$, where v is a 0-1 generator of V, then $f(v)$ corresponds to a minimal zero sum, else $f(v) = u_1 + u_2$ where u_i corresponds to a minimal zero sum.

3.4.3 How to decompose $f(v)$

In some cases, we have to decompose $f(v) = u_1 + u_2$; we explain how to get u_1 and u_2.
Let v be a 0-1 generator of V such that $\|f(v)\| = 2m$. Let $e_1, \ldots, e_n$ be the canonical basis of $\mathbb{R}^n$, we have $f(v) = \sum_{i=1}^{n} x_i e_i = \sum_{j=1}^{2m} x_{i_j} e_{i_j}$ where $x_i = 0$ or 1.
We have to find two zero sums between $b_{i_1}, \ldots, b_{i_{2m}}$. We are going to proceed in the same way as in 3.2.2.
u'_1 and u'_2 are 0-1 vectors in $\mathbb{Z}^{2m}$ and correspond to two different zero sums between $b_{i_1}, \ldots, b_{i_{2m}}$. Let U_v be the lattice generated by u'_1 and u'_2. We remark that we can easily obtain u_1 and u_2 from u'_1 and u'_2.
As before we are going to construct a sequence of lattices $\mathcal{L}_{v,i}$ such that $U_v \subset \mathcal{L}_{v,i+1} \subset \mathcal{L}_{v,i} \subset \mathbb{Z}^{2m}$. We start with $\mathcal{L}_{v,0} = \mathbb{Z}^{2m}$, and now we explain how to get $\mathcal{L}_{v,i+1}$ from $\mathcal{L}_{v,i}$.
Let $\mathcal{L}_v$ be a lattice generated by $w_1, \ldots, w_k$ where $w_i = (w_{i,1}, \ldots, w_{i,2m}) \in \mathbb{Z}^{2m}$, such that $U_v \subset \mathcal{L}_v$. Let $q_{\mathcal{L}_v}$ be the following isomorphism of $\mathbb{Z}$ module.

$$\begin{array}{ccc} q_{\mathcal{L}_v} : \mathcal{L}_v & \longrightarrow & \mathcal{L'}_v \\ w_i & \mapsto & (w_{i,1}, \ldots, w_{i,2m}, \sum_{j=1}^{2m} w_{i,j} \lfloor C\Re(\tilde{b}_{i_j}) \rceil, \\ & & \sum_{j=1}^{2m} w_{i,j} \lfloor C\Im(\tilde{b}_{i_j}) \rceil) \end{array}$$

LEMMA 3.5. *Let $\mathcal{L}_v$ be a lattice such that $U_v \subset \mathcal{L}_v$, and $\mathcal{L'}_v = q_{\mathcal{L}_v}(\mathcal{L}_v)$. Let $\nu_1, \ldots, \nu_k$ be a L.L.L. reduced basis of $\mathcal{L'}_v$ and k_0 be an integer such that: for all $i > k_0$, $\|\nu_i^*\| > M$ where $M = \sqrt{m + [(\frac{1}{2} + C\eta)m]^2}$, then the lattice generated by $q_{\mathcal{L}_v}^{-1}(\nu_1), \ldots, q_{\mathcal{L}_v}^{-1}(\nu_{k_0})$ contains U_v.*

PROOF. Use the same arguments as in 3.1 □

Now the following lemma explains when we have to stop the computation of the sequence of lattices.

LEMMA 3.6. *Let $\mathcal{L}_v$ be a lattice which contains U_v. If $\mathcal{L}_v = U_v$ then $RREF(\mathcal{B}_{\mathcal{L}_v})$ has two rows and each column of R contains precisely one 1 and all other entries are 0.*

PROOF. Use the same arguments as in lemma 3.2. □

4. THE ALGORITHM

We describe our algorithm, then we prove that it terminates and that it computes an absolute factorization.

`Absolute factorization algorithm`
Input: $P(X,Y) \in \mathbb{Q}[X,Y]$ irreducible in $\mathbb{Q}[X,Y]$ monic in Y and $deg_{tot}P(X,Y) = deg_Y P(X,Y) = n$.
Output: An exact absolute factor.

1. Generic change of coordinates: Choose $\lambda \in \mathbb{Z}$, $P(X,Y) := P(X + \lambda Y, Y)$.
2. Choice of the fiber: Choose $x_0 \in \mathbb{R}$.
3. Compute y_i, a_i, b_i with the precision η, $C = \lfloor \frac{1}{\eta} \rfloor$ and l the number of $b_i \in \mathbb{R}$.
4. Sort the b_i as explained in subsection 3.2.1.
5. Set $\mathcal{L} := \mathbb{Z}^{\frac{n+l}{2}}$ with the canonical basis.
6. Compute the L.L.L. reduced basis of $\mathcal{L}'$, delete vectors with a large norm (as in lemma 3.1) and keep k_0 vectors w_i such that $\mathcal{L} := Span(w_1, \ldots, w_{k_0}) \supset V$.
7. Compute $RREF(\mathcal{B}_{\mathcal{L}})$.
8. If $RREF(\mathcal{B}_{\mathcal{L}})$ does not satisfy lemma 3.2, then:
   Either there exists a vector $v = (v_1, \ldots, v_{\frac{n+l}{2}})$ such that v is not a 0-1 vector, and
   $| < v, \overrightarrow{C\lfloor \Re(\tilde{b}) \rceil} > | \leq (\frac{1}{2} + C\eta) \sum_{i=1}^{\frac{n+l}{2}} v_i$. Then go back to 1.
   Or no such vector exists, then set $C := 2C$, $\eta := \frac{1}{C}$ and go back to 6.
9. If $RREF(\mathcal{B}_{\mathcal{L}})$ satisfies lemma 3.2, then:
   (a) Recognize the minimal zero sum vectors as in lemmas 3.3 and 3.4.
   (b) Compute the decomposition $f(v) = u_1 + u_2$ in the same way as in step 6, 7 and 8 with lemmas 3.5 and 3.6.
10. Now we have $r_1, \ldots, r_s$ which are 0-1 vectors. Check that $\|r_1\|^2 = \|r_i\|^2$ $(2 \leq i \leq s)$ and $s\|r_1\|^2 = n$. If it is not the case then go back to 1.
11. Construct $\tilde{P}_i \mod (X - x_0)^3$ $(i = 1, \ldots, s)$.
12. Recognize the exact factors $P_i \mod (X - x_0)^3$ from the approximate $\tilde{P}_i$ $(i = 1, \ldots, s)$.
13. Check that P_1 divides P modulo $(X - x_0)^3$: if P_1 does not divide P then go back to 1.
14. Lift this exact factorization.
15. Check that P_1 divides P: if P_1 does not divide P then go back to 1 else return P_1.

REMARK 4.1.
- *The step 11 is explained in [1].*
- *We explain how to choose η in section 5.*

As we mentioned before we have:

LEMMA 4.2. *If the algorithm terminates then the output is correct.*

PROOF. We just have to show that the factorization we obtained is the absolute factorization. In the algorithm if we obtain V then it is clear that we get the absolute factorization. So here we suppose that we get a lattice $\mathcal{L}$ such that $V \subsetneq \mathcal{L}$ and $RREF(\mathcal{B}_{\mathcal{L}})$ satisfies lemma 3.2. We have to prove that in this case the computed P_1 cannot satisfy

step 15 because there would be too many factors. Indeed, these hypotheses mean that there exists a 0-1 vector v such that v is a generator of V, and $v = a + b$ where $a, b \in \mathcal{L}$ are 0-1 vectors.
If $f(v)$ corresponds to a minimal zero sum then the algorithm gives at least two factors corresponding to a and b instead of just one factor. Thus we cannot get an exact factorization because we have too many factors.
If $f(v) = u_1 + u_2$ and u_i corresponds to a minimal zero sum, then if a or b gives two factors, as before we will get too many factors. Else a gives one factor of degree $\|a\|^2 < \|v\|^2 = m$. Thus we cannot get an exact factorization because we have a factor of bad degree. □

LEMMA 4.3. *The algorithm terminates.*

PROOF. In order to prove that the algorithm terminates we just have to prove that there are only a finite number of situation where we go back to step 1, step 6 and step 9.
► There is a finite number of returns to step 1:
This situation corresponds to the first case of step 8, and the bad case of step 10, step 13 and step 15. The algorithm return to step 1 because we are not in a generic situation. Indeed if $| < v, \overrightarrow{C\lfloor \Re(\tilde{b}) \rceil} > | \leq (\frac{1}{2} + C\eta) \sum_{i=1}^{\frac{n+l}{2}} v_i$ then it is possible that v gives a zero sum between the $\epsilon_i \Re(b_i)$, and then between the b_i. But in this situation v is not a 0-1 vector, so we are not in a generic situation. It is obvious that we are not in a generic situation in the bad case of step 10, step 13 and step 15.
Furthermore, lemmas 3.1 and 3.5 show that we consider only bounded integer relations. Thus theorem 2.1 shows that we just have to avoid a finite number of (x_0, λ_0) to be in a generic situation.
Furthermore after each return to step 6, C increases. Thus after a finite number of step if we are in a generic situation and C is large enough we have:
$| < v, \overrightarrow{\lfloor C\Re(\tilde{b}) \rceil} > | > (\frac{1}{2} + C\eta) \sum_{i=1}^{\frac{n+l}{2}} v_i$. This proves that there are only a finite number of return to step 1.
► There is a finite number of return to step 6 and 9:
By the previous claim, here we can suppose that we are in a generic situation. Thus we just have to show that: if C is large enough then in step 6, $\dim(\mathcal{L})$ decreases. Hence after a finite number of steps we have $V = \mathcal{L}$ (or in step 9, $U_v = \mathcal{L}_v$). Suppose that $\mathcal{L}' = Span(p_{\mathcal{L}}(w_1), \ldots, p_{\mathcal{L}}(w_k))$, then $\det(\mathcal{L}') = \sqrt{\det(< p_{\mathcal{L}}(w_i), p_{\mathcal{L}}(w_j) >)}$. Furthermore $p_{\mathcal{L}}(w_i) = (w_{i,1}, \ldots, w_{i,\frac{n+l}{2}}, < w_i, \overrightarrow{\lfloor C\epsilon\Re(\tilde{b}) \rceil} >)$, thus $\det(\mathcal{L}')$ is a polynomial in C. Let $\nu_1, \ldots, \nu_k$ be a L.L.L. reduced basis of $\mathcal{L}'$, we have $\det(\mathcal{L}') = \prod_{i=1}^{k} \|\nu_i^*\|$. Thus if C is large enough, as $\det(\mathcal{L}')$ is a polynomial there exist an index k_0 such that
$\|\nu_{k_0}^*\| > \sqrt{\frac{n+l}{2} + [(\frac{1}{2} + C\eta) + \frac{n+l}{2}]^2}.2^{\frac{n+l}{2}} = \mathcal{M}$. (It is important to remember that $C\eta \leq 1$.) Hence $\mathcal{M} \leq \|\nu_{k_0}^*\| \leq 2^{\frac{i}{2}} \|\nu_{k_0+i}^*\|$ $(1 \leq i \leq \frac{n+l}{2} - k_0)$, see proposition 2.6, and then $\sqrt{\frac{n+l}{2} + [(\frac{1}{2} + C\eta) + \frac{n+l}{2}]^2} \leq \mathcal{M}.2^{\frac{-i}{2}} \leq \|\nu_{k_0+i}^*\|$, $(1 \leq i \leq \frac{n+l}{2} - k_0)$. Thus, the dimension of $\mathcal{L}'$ decreases and then the dimension of $\mathcal{L}$ decreases. This proves the second claim. □

5. COMMENTS AND OPTIMIZATIONS

First we present an heuristic which gives the precision η in the step 3 of the algorithm. Second, we recall some results about the number of real roots of a polynomial, in order to estimate the size of the number l. Third, we propose two improvements of the step 6 of the algorithm. Finally, we briefly estimate the complexity of the algorithm.

5.1 How to choose η

First, we explain why we set $C = \lfloor \frac{1}{\eta} \rfloor$. We have $|\tilde{b}_i - b_i| < \eta$, then $|C\Re(\tilde{b}_i) - C\Re(b_i)| < C\eta$. As we study the integral part of these numbers, we want $C\eta < 1$. But if $C\eta << 1$, that means that when we take the integral part we do not use all the "exact information" of the decimal part. Thus the optimal choice is $C\eta = 1$, and as we want that C belongs to $\mathbb{Z}$, we choose $C = \lfloor \frac{1}{\eta} \rfloor$.
Now we want to choose η (thus C), in such a way that $RREF(\mathcal{B}_{\mathcal{L}})$ satisfies lemma 3.2. That is to say we do not want to return to step 6, after the step 8. Thus let $\nu_1, \ldots, \nu_{\frac{n+l}{2}}$ be a L.L.L. reduced basis of $\mathcal{L}'$, where $\mathcal{L} = \mathbb{Z}^{\frac{n+l}{2}}$ with the canonical basis. An heuristic says that the vectors ν_i are near orthogonal. By this heuristic:
$\prod_{i=1}^{\frac{n+l}{2}} \|\nu_i^*\| \approx \prod_{i=1}^{\frac{n+l}{2}} \|\nu_i\|$. Furthermore $\prod_{i=1}^{\frac{n+l}{2}} \|\nu_i^*\| = \det(\mathcal{L}')$ $= \sqrt{\det(A)}$. A is the $\frac{n+l}{2} \times \frac{n+l}{2}$ symmetric matrix such that $A_{i,i} = 1 + [C\lfloor \epsilon_i \Re(\tilde{b}_i) \rceil]^2$, and $A_{i,j} = C^2 \epsilon_i \epsilon_j \lfloor \Re(\tilde{b}_i) \rceil \lfloor \Re(\tilde{b}_j) \rceil$ if $i \neq j$. For computing an estimate of C we replace $\lfloor \epsilon_i \Re(\tilde{b}_i) \rceil$ by one. That means that we do not study the determinant of the matrix A, but the determinant of the matrix B where B is the $\frac{n+l}{2} \times \frac{n+l}{2}$ matrix such that $B_{i,i} = 1 + C^2$, and $B_{i,j} = C^2$ if $i \neq j$. Finally we have
$\sqrt{\det B} \approx \prod_{i=1}^{\frac{n+l}{2}} \|\nu_i\|$. Furthermore $\det B = 1 + (\frac{n+l}{2})C^2$, and we want that here is a gap i.e. either
$\|\nu_i\| \approx \sqrt{\frac{n+l}{2} + [(\frac{1}{2} + C\eta)\frac{n+l}{2}]^2}$ for the ones we will keep, or $\|\nu_i\| > \sqrt{\frac{n+l}{2} + [(\frac{1}{2} + C\eta)\frac{n+l}{2}]^2}$ for the ones we delete. Thus we get: $1 + \frac{n+l}{2}C^2 \geq (\frac{n+l}{2} + [(\frac{1}{2} + C\eta)\frac{n+l}{2}]^2)^{\frac{n+l}{2}}$, it follows:

$$C \geq \frac{\sqrt{2}}{\sqrt{n+l}} \sqrt{\left(\frac{n+l}{2} + [\frac{3}{4}(n+l)]^2\right)^{\frac{n+l}{2}} - 1}.$$

5.2 How many b_i are real?

Here we just recall a result about the number of real roots of a polynomial with real coefficients. We have the following result (see [10] or [6]).

THEOREM 5.1. *For a random polynomial $a_0 + a_1 x + \ldots + a_n x^n$, where the a_i are independent standard normals; the expected number of real zeros E_n satisfies when $n \to \infty$:*

$$E_n = \frac{2}{\pi} \log(n) + 0.62573... + \frac{2}{n\pi} + O(\frac{1}{n^2}).$$

If the random variables a_i are independent normal with mean zero, but the variance of a_i is equal to $\binom{n}{i}$, then these random polynomials have $E_n = \sqrt{n}$ real zero on average.

As b_i are conjugate algebraic numbers, with this theorem we can suppose that in general l is very small compare to n. We deduce then: $\frac{n+l}{2} < n$, so it is much better to apply

the L.L.L. algorithm to a dimension $\frac{n+l}{2}$ lattice than to a dimension n lattice. This explains why we study the real part of b_i instead of b_i.

5.3 First optimization

Here we explain how to improve step 6 of the algorithm. Indeed it is possible that $k_0 = k$ and that the first vectors $w_1, \ldots, w_{k_1}$ are 0-1 vectors (see section 6 where $k_0 = \frac{n+l}{2} = 62$ and $k_1 = 4$). In this case if we are in a generic situation with a large constant C and $| < w_1, \overrightarrow{\lfloor C\epsilon\Re(\tilde{b})\rceil} > | \leq (\frac{1}{2} + C\eta)\|w_1\|$ then $< w_1, \overrightarrow{\epsilon\Re(b)} >= \sum_{i\in I} \epsilon_i \Re(b_i) = 0$. That means that we have a zero sum between the $\epsilon_i\Re(b_i)$ (where $i \in I$), and we want to decompose it. So we apply our L.L.L. strategy to the set $\{\epsilon_i\Re(b_i)/i \in I\}$.
In conclusion, if we get k_1 0-1 vectors we can split our problem into k_1 smaller zero sum problems.

5.4 Second optimization

Here we explain how to improve step 6 of the algorithm. In section 3.2 and 3.4 we showed how to use the L.L.L. algorithm in order to obtain minimal zero sum relations. But the matrix $(\mathcal{B}_{\mathcal{L}'})$ is not square, and it would be better to have a square matrix. First, we remark that when $\mathcal{L} = \mathbb{Z}^{\frac{n+l}{2}}$ with its canonical basis, then $RREF(\mathcal{B}_{\mathcal{L}'})$ is the identity matrix. Secondly, we remark that in the other cases we have $\mathcal{L}$, and $RREF(\mathcal{B}_{\mathcal{L}})$ too. Now, we explain how to use the informations given by $RREF(\mathcal{B}_{\mathcal{L}})$ in order to get a lattice $\mathcal{L}''$ such that $(\mathcal{B}_{\mathcal{L}''})$ is square.
We set $\mathcal{L} = Span(w_1, \ldots, w_k) \subset \mathbb{Z}^{\frac{n+l}{2}}$. c_i is the i^{th} column of $RREF(\mathcal{B}_{\mathcal{L}})$. $\mathfrak{C} = \{i_1, \ldots, i_k\}$ is the set of indices such that c_{i_j} is the column with j^{th} coordinate equal to 1 and all the others coordinates equal to 0. Then for all $i \in \{1, \ldots, n\} - \mathfrak{C}$, $c_i, c_{i_1}, \ldots, c_{i_k}$ are linearly dependents, and if

$$c_i = \begin{pmatrix} \theta_{i,1} \\ \vdots \\ \theta_{i,k} \end{pmatrix} \text{ then } c_i = \sum_{j\in\mathfrak{C}} \theta_{i,j} c_j \quad (*).$$

That means that if we know the $i_1, \ldots, i_k$ coordinates of w_1 then with the formula $(*)$ we can recover all the coordinates of w_1.
Let us use these relations between the c_i. We consider the map:

$$\begin{array}{rcl} r_{\mathcal{L}} : \mathcal{L} & \longrightarrow & \mathcal{L}'' \\ w_i = (w_{i,1}, \ldots, w_{i,\frac{n+l}{2}}) & \mapsto & (w_{i,i_1}, \ldots, w_{i,i_{k-1}}, \\ & & < w_i, \overrightarrow{\lfloor C\epsilon\Re(\tilde{b})\rceil} >) \end{array}$$

This is an isomorphism of $\mathbb{Z}$ module.

In this situation, the following lemma is the equivalent of lemma 3.1, but here $\mathcal{L}'' = r_{\mathcal{L}}(\mathcal{L})$ provides a square matrix $(\mathcal{B}_{\mathcal{L}''})$.

LEMMA 5.2. *Let $\mathcal{L}$ a lattice of dimension k such that $V \subset \mathcal{L}$, and $\mathcal{L}'' = r_{\mathcal{L}}(\mathcal{L})$. Let $\nu_1, \ldots, \nu_k$ be a L.L.L. reduced basis of $\mathcal{L}''$ and k_0 an integer such that:*
for all $i > k_0$, $\|\nu_i^*\| > M$ where $M = \sqrt{k - 1 + [(\frac{1}{2} + C\eta).k]^2}$.
Then the lattice generated by $r_{\mathcal{L}}^{-1}(\nu_1), \ldots, r_{\mathcal{L}}^{-1}(\nu_{k_0})$ contains V.

We can also adapt this idea to step 9b. of the algorithm.

5.5 Complexity analysis and future challenge

5.5.1 Theoretical complexity

The number of bit operations needed by step 6 is the bottleneck of our algorithm. With the second optimization we can suppose that we have k vectors $v_i \in \mathbb{Z}^k$, and that $\|v_i\| \approx C$. We know (see [14]) that the number of bits operations needed by the L.L.L. algorithm is $O(k^{5+\epsilon}(\log C)^{2+\epsilon})$ for every $\epsilon > 0$, if we employ fast multiplication algorithm. Furthermore at the beginning of the algorithm we have $k = \frac{n+l}{2}$ and $C \geq \frac{n+l}{2}^{\frac{n+l}{2}}$ see 5.1. Then the number of bits operations needed by the L.L.L. algorithm to perform step 6 is $O(n^{7+\epsilon} \log^{2+\epsilon} n)$.

5.5.2 Practical complexity

In practice our algorithm already allows us to factorize polynomials of total degree 200, we present hereafter an illustrative example of degree 120. The challenge problem seems to be: Can we compute a certified absolute polynomial factorization of an irreducible polynomial in $\mathbb{Q}[X, Y]$ of total degree bigger than 500?

6. SKETCH OF AN EXAMPLE

Here we follow our algorithm with PARI/GP Version 2.1.4, on a polynomial $P(X, Y)$. $P(X, Y)$ has the following properties: $P(X, Y) \in \mathbb{Z}[X, Y]$ is monic in Y and is irreducible in $\mathbb{Q}[X, Y]$. Furthermore P has 1268 monomials, the average size of the coefficients is 5.10^7, and the biggest coefficient is approximatively 3.10^9 (see http://math.unice.fr/ cheze/).

Step 1: We choose $\lambda = 0$.
Step 2: We choose $x_0 = 1$.
Step 3: Four b_i belongs to $\mathbb{R}$, then $C \geq 10^{121}$. We set 150 significant digits for our computation, and $C = 10^{130}$.
Step 4: We sort the b_i.
Step 5: $\mathcal{L} = \mathbb{Z}^{62}$ with its canonical basis.
Step 6: We compute the L.L.L. reduced basis of $\mathcal{L}'$. We compute M (see lemma 3.1), we get $M \approx 93$. It follows $k_0 = 62$, because $\|w_{62}^*\| \approx 53$. But, for $i = 1, \ldots, 4$, $\|w_i^*\| \leq 93$, and w_i are 0-1 vectors. So we apply the first optimization:
`First optimization:`
w_1 has 10 coordinates equal to 1, and all the other are 0. We set $\mathcal{L}_{opt} = \mathbb{Z}^{10}$, and we compute $\{w_{opt\,1}, \ldots, w_{opt\,10}\}$ the L.L.L. reduced basis of $\mathcal{L}'_{opt}$. We compute $M_{opt} = \sqrt{10 + (\frac{3}{2}.10)^2}$, we get $M_{opt} \approx 15$. It follows $k_0 = 1$, because for all $i \geq 2$, we have $\|w_{opt\,i}^*\| \geq 10^{14} > 15$.
All the coordinates of $w_{opt\,1}$ are equal to 1. Then we deduce that w_1 is a minimal zero sum between the $\epsilon_i\Re(b_i)$. As $\|f(w_1)\|^2 = 20 = \|f(w_2)\|^2$, $\|f(w_3)\|^2 = \|f(w_4)\|^2 = 40$, and $w_{2,1} = w_{2,2} = w_{2,3} = w_{2,4} = 1$, we deduce: $f(w_1)$, $f(w_2)$ give minimal zero sums between the b_i, $f(w_3)$ gives two minimal zero sums between the b_i, and $f(w_4)$ gives two minimal zero sums between the b_i.
Step 7,8: Using the first optimization, we have $\mathcal{L} = Span(w_1, \ldots, w_4)$ and then $RREF(\mathcal{B}_{\mathcal{L}})$ satisfies lemma 3.2.
Step 9: We have to decompose $f(w_3)$ and $f(w_4)$. We set $\mathcal{L}_{w_3} = \mathbb{Z}^{40}$, and we compute $\{w_{w_3\,1}, \ldots, w_{w_3\,40}\}$ the L.L.L. reduced basis of $\mathcal{L}'_{w_3}$. We compute M_{w_3}, we get $M_{w_3} \approx 30$. It follows $k_0 = 2$, because for all $i \geq 3$, $\|w_{w_3\,i}^*\| \geq 10^6 > 30$, and the first two vectors $w_{w_3\,1}^*$, $w_{w_3\,2}^*$ are 0-1 vectors.

We obtain the same results for $f(w_4)$.
Step 10: We get 6 vectors r_i (for example $r_1 = f(w_1), r_2 = f(w_2)$), such that $\|r_i\|^2 = 20$, then $s = 6$ and $s.\|r_i\|^2 = 120$.
Step 11: $\tilde{P}_i = \prod_{j \in J_i}(Y - \tilde{y}_j - \tilde{a}_j(X-1) - \tilde{b}_j(X-1)^2) \bmod (X-1)^3$, where J_i is the set of indices such that: j belongs to J_i if the j^{th} coordinates of r_i is 1.
Step 12,13: We recognize the exact factors of P, and we get P_1 divides P modulo $(X-1)^3$.

REMARK 6.1. *If we do not follow the first optimization, we have to compute a L.L.L. reduced basis of a dimension 62 lattice. With the first optimization we avoid this computation, we only compute a L.L.L. reduced basis of a dimension 10 lattice.*

7. ACKNOWLEDGMENT

The author thanks Guillaume Hanrot, Paul Zimmermann and André Galligo for their helpful comments and discussions.

8. REFERENCES

[1] G. CHÈZE AND A. GALLIGO, *From an approximate to an exact factorization*. Submitted to JSC, 2003.

[2] ——, *Four lessons on polynomial absolute factorization*, 2004. To appear in a CIMPA School book.

[3] R. CORLESS, A. GALLIGO, I. KOTSIREAS, AND S. WATT, *A geometric-numeric algorithm for factoring multivariate polynomials*, in Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC 2002), T. Mora, ed., ACM, 2002, pp. 37–45.

[4] O. CORMIER, M. F. SINGER, B. M. TRAGER, AND F. ULMER, *Linear differential operators for polynomial equations*, J. Symbolic Comput., 34 (2002), pp. 355–398.

[5] D. DUVAL, *Absolute factorization of polynomials: a geometric approach*, SIAM J. Comput., 20 (1991), pp. 1–21.

[6] A. EDELMAN AND E. KOSTLAN, *How many zeros of a random polynomial are real?*, Bull. Amer. Math. Soc. (N.S.), 32 (1995), pp. 1–37.

[7] A. GALLIGO, *Real factorization of multivariate polynomials with integer coefficients*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI), 258 (1999), pp. 60–70, 355.

[8] A. GALLIGO AND D. RUPPRECHT, *Irreducible decomposition of curves*, J. Symbolic Comput., 33 (2002), pp. 661–677. Computer algebra (London, ON, 2001).

[9] S. GAO, *Factoring multivariate polynomials via partial differential equations*, Math. Comp., 72 (2003), pp. 801–822 (electronic).

[10] M. KAC, *On the average number of real roots of a random algebraic equation*, Bull. Amer. Math. Soc., 49 (1943), pp. 314–320.

[11] E. KALTOFEN, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization*, SIAM J. Comput., 14 (1985), pp. 469–489.

[12] ——, *Polynomial factorization 1987–1991*, in LATIN '92 (São Paulo, 1992), vol. 583 of Lecture Notes in Comput. Sci., Springer, Berlin, 1992, pp. 294–313.

[13] ——, *Effective Noether irreducibility forms and applications*, J. Comput. System Sci., 50 (1995), pp. 274–295. 23rd Symposium on the Theory of Computing (New Orleans, LA, 1991).

[14] A. K. LENSTRA, H. W. LENSTRA, JR., AND L. LOVÁSZ, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 515–534.

[15] K. NAGASAKA AND T. SASAKI, *Approximate factorization of multivariable polynomials and its computational complexity*, Sūrikaisekikenkyūsho Kōkyūroku, (1998), pp. 111–118. Research on the theory and applications of computer algebra (Japanese) (Kyoto, 1997).

[16] D. RUPPRECHT, *Elements de géométrie algébrique approchée: Etude du pgcd et de la factorisation*, PhD thesis, Univ. Nice Sophia Antipolis, 2000.

[17] T. SASAKI, *Approximate multivariate polynomial factorization based on zero-sum relations*, in Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (ISSAC 2001), B. Mourrain, ed., ACM, 2001, pp. 284–291.

[18] T. SASAKI, M. SUZUKI, M. KOLÁŘ, AND M. SASAKI, *Approximate factorization of multivariate polynomials and absolute irreducibility testing*, Japan J. Indust. Appl. Math., 8 (1991), pp. 357–375.

[19] A. SOMMESE, J. VERSCHELDE, AND C. WAMPLER, *Symmetric functions applied to decomposing solution sets of polynomial systems*, SIAM J. Numer. Anal., 40 (2002), pp. 2026–2046.

[20] ——, *Numerical factorization of multivariate complex polynomials*. Accepted for publication in a special issue of *Theoretical Computer Science* on Algebraic and Numerical Algorithms, 2003.

[21] B. TRAGER, *On the integration of algebraic functions*, PhD thesis, M.I.T., 1985.

[22] C. TRAVERSO, *A study on algebraic algorithms: the normalization*, Rend. Sem. Mat. Univ. Politec. Torino, (1986), pp. 111–130 (1987). Conference on algebraic varieties of small dimension (Turin, 1985).

[23] M. VAN HOEIJ, *Factoring polynomials and the knapsack problem*, J. Number Theory, 95 (2002), pp. 167–189.

[24] J. VON ZUR GATHEN, *Irreducibility of multivariate polynomials*, J. Comput. System Sci., 31 (1985), pp. 225–264. Special issue: Twenty-fourth annual symposium on the foundations of computer science (Tucson, Ariz., 1983).