ALGEBRAIC OSCULATION AND FACTORIZATION OF SPARSE POLYNOMIALS

MARTIN WEIMANN

Abstract. We prove a theorem on algebraic osculation and we apply our result to the Computer Algebra problem of polynomial factorization. We consider X a smooth completion of $\mathbb{C}^2$ and D an effective divisor with support $\partial X = X \setminus \mathbb{C}^2$. Our main result gives explicit conditions equivalent to that a given Cartier divisor on the subscheme $(|D|, \mathcal{O}_D)$ extends to X. These osculation criterions are expressed with residues. We derive from this result a toric Hensel lifting which permits to compute the absolute factorization of a bivariate polynomial by taking in account the geometry of its Newton polytope. In particular, we reduce the number of possible recombinations when compared to the Galligo-Rupprecht algorithm.

1. Introduction

This article is originally motivated by the wellknown Computer Algebra problem of polynomial factorization. We introduce here a new method to compute the absolute factorization of sparse bivariate polynomials, which is based on criterions for algebraic osculation in toric varieties.

Since the eightees, several deterministic or probabilistic algorithms have been obtained to compute the irreducible absolute factorization of dense bivariate polynomials defined over a number field $K \subset \mathbb{C}$. We refer the reader to [17] and [9] for a large overview of the subject. In many cases, these algorithms are based on a *Lifting and Recombination* scheme - refered here under the generical term LR-algorithms - which mainly consists to detect irreducible absolute factors of a polynomial $f \in K[t_1, t_2]$ in its formal decomposition in $\bar{K}[[t_1]][t_2]$. Although this approach *a priori* necessites an exponential number of possible recombinations, people succeded in the last decade to develop LR-algorithms running now in a quasi-optimal polynomial complexity (see for instance [8], [1], [9] and the reference within).

In general, a LR-algorithm first performs a generic affine change of coordinates. When f has many zero coefficients in its dense degree d monomial expansion - we say that f is *sparse* - this step loses crucial information. In this article, we propose a new method which avoids this generical choice of coordinates. Roughly speaking, we obtain a toric version of the Hensel lifting process (in the spirit of [1]) which detects and computes the irreducible absolute factors of f by taking in account the geometry of its Newton polytope N_f. This permits in particular to reduce the number of possible recombinations when compared to the Galligo-Rupprecht algorithm [13].

Let us present our main results.

Algebraic Osculation. A natural way to profit from the Newton polytope information is to embed the complex curve of f in a smooth toric compactification X of the complex plane. For a well chosen X, we can recover N_f (up to translation) from the Picard class of the Zariski closure $C \subset X$ of the affine curve of f. The boundary $\partial X = X \setminus \mathbb{C}^2$ of X is a normal crossing divisor whose Picard group satisfies

$$Pic(\partial X) \simeq Pic(X).$$

Thus, it's natural to pay attention to the restriction of C to some effective Cartier divisor D (more precisely, to the subscheme $(|D|, \mathcal{O}_D)$) with support $|\partial X|$. In order to detect the irreducible components of C, we need to find conditions for that a Cartier divisor on D extends to X. This is achieved in our main

Theorem 1. *Let X be a smooth projective compactification of $\mathbb{C}^2$, whose boundary $\partial X = X \setminus \mathbb{C}^2$ is a normal crossing divisor. Let D be an effective Cartier divisor with support $|\partial X|$ and let $\Omega^2_X(D)$ be the sheaf of meromorphic 2-forms with polar locus bounded by D.*

There exists a pairing $\langle \cdot, \cdot \rangle$ between the group of Cartier divisors on D and the vector space $H^0(X, \Omega^2_X(D))$ with the property that a Cartier divisor γ on D extends to a Cartier divisor E on X if and only if

$$\langle \gamma, \Psi \rangle = 0 \quad \forall\ \Psi \in H^0(X, \Omega^2_X(D)).$$

The divisor E is unique up to rational equivalence.

Not surprisingly, we'll construct such a pairing by using Grothendieck residues (see for instance [21] where the authors study the interplay between residues and zero-dimensional subschemes extension). When X is a toric surface we obtain an explicit formula for $\langle \gamma, \Psi \rangle$, generalizing a theorem of Wood [34]. To prove Theorem 1, we compute the cohomological obstruction to extend line bundles from D to X and then we use the Dolbeault $\bar{\partial}$-resolution and residue currents to make explicit the conditions.

Application to polynomial factorization. If two algebraic curves of fixed degree osculate each other on a finite subset with sufficiently big contact orders, they necessarily have a common component. This basic observation permits to derive from Theorem 1 a sketch of algorithm which computes the absolute factorizion of a bivariate polynomial f. The polynomial f is assumed to be defined over a subsfield $K \subset \mathbb{C}$ and we look for its irreducible decomposition over $\mathbb{C}$.

Under the assumption $f(0) \neq 0$, we can associate to f a smooth toric completion X of $\mathbb{C}^2$ whose boundary

$$\partial X = D_1 + \cdots + D_r$$

is a normal crossing toric divisor and such that the curve $C \subset X$ of f does not contain any torus fixed points of X. A Minkowski sum decomposition

$$N_f = P + Q$$

of the Newton polytope of f corresponds to a line bundle decomposition

$$\mathcal{O}_X(C) \simeq \mathcal{L}_P \otimes \mathcal{L}_Q,$$

where $\mathcal{L}_P$ and $\mathcal{L}_Q$ are both globally generated with at least one non trivial global section.

We obtain the following result

Theorem 2. *There exists an unique effective divisor D with support $|\partial X|$ and rationally equivalent to $C + \partial X$. Let γ be the restriction of C to D and suppose that $N_f = P + Q$. There exists an absolute factor q of f with Newton polytope Q if and only if there exists $0 \leq \gamma' \leq \gamma$ such that*

$$deg(\gamma' \cdot D_i) = deg\, \mathcal{L}_{Q|D_i}, \quad i = 1, \ldots, r$$

and so that the osculation conditions hold for the pair (D, γ'). The factor q can be explicitely computed from γ' by solving a sparse linear system of $2 \times Vol(Q)$ equations and $Card(Q \cap \mathbb{Z}^2)$ unknowns.

When the facet polynomials of f are square free over $\bar{K}$, we can derive from Theorem 2 the sketch of a vanishing-sum LR-algorithm (Subsection 3.4). It first computes the Newton polytope decomposition

$$N_f = Q_1 + \cdots + Q_s$$

associated to the absolute decomposition of f. Then it computes the associated irreducible absolute factorization

$$f = q_1 \times \cdots \times q_s$$

with floatting calculous and with a given precision. The numerical part of our algorithm reduces to the absolute factorization of the univariate exterior facet polynomials and the algorithmic complexity depends now on the Newton polytope N_f instead of the usual degree $d = deg(f)$. In particular, we fully profit from the combinatoric restrictions imposed by Ostrowski's conditions $N_{pq} = N_p + N_q$ (see [28]). This permits to reduce the number of possible recombinations when compared to the Galligo-Rupprecht algorithm [13].

Finally, let us mention that Theorem 1 concerns also non toric $\mathbb{C}^2$-completions. In theory, this permits to exploit the information given by the *non toric* singularities of C along the boundary of X when f has non reduced facet polynomials (see Subsection 3.6).

A formal study of algorithmic complexity, as well as questions of using non toric singularities information will be explored in a further work.

Related results. Our method is inspired by an algorithm presented in [12] that uses generical toric interpolation criterions [32] in an open neighborhood of ∂X (see Subsection 3.5). By using combinatorics tools, the authors in [1] obtain a comparable Hensel lifting process which there too takes in account the geometry of the Newton polytope. Finally, let us mention [3], where the authors reduce the factorization of a sparse polynomial to smaller dense factorizations.

Organization. The article is organized as follow. Section 2 is devoted to Algebraic Osculation. We introduce the problem in Subsection 2.1 and we construct the residue pairing in Subsection 2.2. We enounce precisely Theorem 1 in Subsection 2.3 and we give the proof in Subsection 2.4. We give an explicit formula for the osculation criterions when X is a toric surface in Subsection 2.5. In Section 3, we pay attention to polynomial factorization. We prove Theorem 2 in Subsections 3.2 and 3.3 and we develop the sketch of a sparse polynomial factorization algorithm

in Subsection 3.4. We compare the underlying algortihmic complexity with related results in Subsections 3.5 and discuss non toric information in Subsection 3.6. We conclude in the last Subsection 3.7.

Aknowledgment. We would like to thanks Michel Brion, Stéphane Druel, José Ignacio Burgos and Martin Sombra for their disponibility and helpfull comments. We thanks Mohamed Elkadi and André Galligo who suggested me to pay attention to sparse polynomial factorization.

2. Algebraic osculation

We prove here our main result giving criterions for algebraic osculation on the boundary of a smooth projective completion of the complex plane. In Subsection 2.5, we make explicit the osculation criterions in the toric case.

2.1. **Notations and motivation.** In all the sequel, $(X, \mathcal{O}_X)$ designs a smooth projective surface where

$$X = X_0 \sqcup |\partial X|$$

is the disjoint union of an affine surface $X_0 \simeq \mathbb{C}^2$ and of the support of a simple normal crossing divisor

$$\partial X = D_1 + \cdots + D_r.$$

We say that X is a completion of the complex plane with boundary ∂X.

An *osculation data* on the boundary of X is a pair (D, γ) where

$$D = (k_1 + 1)D_1 + \cdots + (k_r + 1)D_r$$

is an effective divisor with support $|D| = |\partial X|$ and γ is a Cartier divisor on the subscheme $(|D|, \mathcal{O}_D)$. By abuse of language, we'll write $D = (|D|, \mathcal{O}_D)$.

An *osculating divisor* for (D, γ) is a Cartier divisor E on X which restricts to γ on D. That is

$$i^*(E) = \gamma,$$

where $i : D \to X$ is the inclusion map. In other words, we are looking for a divisor E with prescripted restriction to the k_i^{th}-infinitesimal neighborhood of D_i. In general, such an osculating divisor does not exist and we are interested here to determine the necessary extra conditions.

We say that γ has support $|\Gamma|$, where Γ designs the zero-cycle $\gamma \cdot \partial X$. Thus, γ can be uniquely written as a finite sum

$$\gamma = \sum_{p \in |\Gamma|} \gamma_p,$$

each γ_p being the restriction to D of a germ of an analytic *cycle* of X

$$\widetilde{\gamma}_p = div(f_p)$$

at p. If p belongs to the smooth part of the boundary and $\widetilde{\gamma}_p$ is irreducible, a curve restricts to γ_p at p if and only if it has contact order at least k_p with $\widetilde{\gamma}_p$, where $k_p + 1$ is the multiplicity of D at p. This observation motivates the terminology of algebraic osculation.

2.2. **Residues.** It's a classical fact that Grothendieck residues play a crucial role in osculation and interpolation problems. Let us mention for instance [19], [23], [31] and [32] for interpolation results and [21] for the interplay between residues and subscheme extensions. Not surprisingly, residues will appear here too.

Let Ω^2_X be the canonical bundle of X. We identify the line bundle $\Omega^2_X(D)$ with the sheaf of meromorphic forms with polar locus bounded by D. Thus, any global section Ψ of $\Omega^2_X(D)$ restricts to a closed 2-form on X_0. Since $X_0 \simeq \mathbb{C}^2$ is simply connected, there exists a rational 1-form ψ on X such that

$$d\psi_{|X_0} = \Psi_{|X_0}.$$

For $p \in |\Gamma|$, we denote by ψ_p the germ of ψ in the chosen local coordinates. Let h_p be a local equation of D at p. Thus $h_p\psi_p$ is holomorphic at p. Suppose for a while that f_p is holomorphic and irreducible. Then, following [20], we define the Grothendieck residue at p of the germ of meromorphic two form $df_p \wedge \psi_p/f_p$ as

$$res_p\left[\frac{df_p}{f_p} \wedge \psi_p\right] := \lim_{\underline{\epsilon}\to 0} \frac{1}{(2i\pi)^2} \int_{u_p(\epsilon)} \frac{df_p}{f_p} \wedge \psi_p, \tag{1}$$

where $u_p(\epsilon) = \{x \text{ close to } p,\ |f_p(x)| = \epsilon_1, |h_p| = \epsilon_2\}$.

This definition does not depend on the choice of local coordinates [20]. By Stokes Theorem, it only depends on $d\psi = \Psi$. Moreover, the local duality Theorem [20] implies that (1) only depends on f_p modulo (h_p). That is, (1) depends on γ_p and not on the chosen lifting $\widetilde{\gamma}_p = \{f_p = 0\}$. By linearity, we can extend (1) to any germ of analytic cycle $\widetilde{\gamma}_p = div(f_p)$. Finally, we deduce that (1) defines a bilineary operator

$$\langle \gamma, \Psi\rangle_p := res_p\left[\frac{df_p}{f_p} \wedge \psi_p\right]$$

between the group of Cartier divisor of D and the $\mathbb{C}$-vector space $H^0(X, \Omega^2_X(D))$. We refer to the proof of Theorem 1 (Subsection 2.4) for more details.

2.3. **Criterions for algebraic osculation.** We keep previous notations. Our main result is the following

Theorem 1. *Let (D, γ) be an osculating data on the boundary of X.*

1. There exists a Cartier divisor E on X which restricts to γ if and only if

$$\sum_{p\in|\Gamma|} \langle \gamma, \Psi\rangle_p = 0 \ \ for\ \ all\ \ \Psi \in H^0(X, \Omega^2_X(D)). \tag{2}$$

The divisor E is unique up to rational equivalence.

2. If moreover γ is effectif and

$$H^1(X, \mathcal{O}_X(E - D)) = 0,$$

then there exists an effective divisor of X which restricts to γ on D.

The necessity of (2) follows from the Residue Theorem [20]. The difficult part consists to show sufficiency of conditions. The proof will be given in the next Subsection 2.4.

Let us first illustrate Theorem 1 on a simple example.

Example 1 (the Reiss relation). Let $X = \mathbb{P}^2$ and consider a finite collection of $d > 0$ *smooth* analytic germs $\widetilde{\gamma}_p$ transversal to a line $L \subset \mathbb{P}^2$. Suppose that we look for an algebraic curve $C \subset \mathbb{P}^2$ of degree d which osculates each germ with a contact order ≥ 2. This problem leads to the osculation data (D, γ), where $D = 3L$ and γ is the restriction to D of $\sum_{p \in |\Gamma|} \widetilde{\gamma}_p$. There is an isomorphism

$$H^0(\mathbb{P}^2, \Omega^2_{\mathbb{P}^2}(3L)) \simeq H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}) \simeq \mathbb{C}$$

and we can check that the form Ψ whose restriction to $\mathbb{C}^2 = \mathbb{P}^2 \setminus L$ is given by $\Psi_{|\mathbb{C}^2} = dx_0 \wedge dy_0$ is a generator. Thus we can choose $\psi_{|\mathbb{C}^2} = x_0 dy_0$. Letting $x_0 = X/Z$ and $y_0 = Y/Z$ we obtain

$$\psi = \frac{X(ZdY - YdZ)}{Z^3}$$

in the $\mathbb{P}^2$ homogeneous coordinates $[X : Y : Z]$. Up to an affine change of coordinates, we can suppose that γ is supported in the affine chart $Y \neq 0$. In the new affine coordinates $x = Z/Y$ and $y = X/Y$, the line L has local equation $x = 0$ and $\psi = ydx/x^3$. Moreover, we can choose a Weierstrass equation

$$\widetilde{\gamma}_p = y - \phi_p(x)$$

for the smooth germ $\widetilde{\gamma}_p$, where $\phi_p \in \mathbb{C}\{x\}$. By Cauchy formula, we obtain

$$res_p\Big[\frac{ydx \wedge d(y - \phi_p)}{x^3(y - \phi_p)}\Big] = res_0\Big[\phi_p(x)\frac{dx}{x^3}\Big] = \frac{1}{2}\phi_p''(0),$$

where res_0 is an univariate residue and ϕ_p'' is the second derivative of ϕ_p. Finally, (2) is here equivalent to that

$$\sum_{p \in |\Gamma|} \phi_p''(0) = 0. \tag{3}$$

For degree reasons, any osculating divisor is rationally equivalent to dL and by Serre duality

$$H^1(\mathcal{O}_{\mathbb{P}^2}(d-3)) \simeq H^0(\mathcal{O}_{\mathbb{P}^2}(-d)) = 0.$$

Thus (3) is the unique relation necessary for that there exists an osculating curve C for (D, γ).

It's easy to see directly necessity of (3). An osculating curve is given by a degree d polynomial $C = \{f(x, y) = 0\}$ that can be factorized

$$f(x, y) = \prod_{p \in |\Gamma|} (y - u_p(x))$$

in $\mathbb{C}\{x\}[y]$. Since $deg(f) = d$, the sum $\sum_{p \in |\Gamma|} u_p(x)$ is a degree 1 polynomial and the relation

$$\sum_{p \in |\Gamma|} u_p''(0) = 0$$

holds. If C osculates $\widetilde{\gamma}_p$ with contact oder 2, then ϕ_p and u_p have the same Taylor expansion up to order 2, which directly shows necessity of (3). When we express the second derivative of u_p in terms of the partial derivative of f, we recover the classical Reiss relation [18]. This result is obtained by Griffiths-Harris in [20], Chapter 6.

2.4. **Proof of Theorem 1.** The Cartier divisor γ on D corresponds to a line bundle $\mathcal{L} \in Pic(D)$ over D together with a global meromorphic section f. An osculating divisor for (D, γ) corresponds to a line bundle $\widetilde{\mathcal{L}} \in Pic(X)$ together with a global meromorphic section $\widetilde{f}$ which restrict respectively to $\mathcal{L}$ and f on D.

The following lemma gives the formal cohomological obstruction for the extension of $\mathcal{L}$. All sheaves are considered here as analytic sheaves and any sheaf on a subscheme $Y \subset X$ is implicitly considered as a sheaf on X by zero extension.

Lemma 1. *There is a decomposition of $Pic(D)$ in a direct sum*

$$Pic(D) = Pic(X) \oplus H^1(D, \mathcal{O}_D).$$

Proof. The classical exponential exact sequence exists for any curve of X (reduced or not, see [5] p.63). We obtain the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_X & \longrightarrow & \mathcal{O}_X & \stackrel{exp(2i\pi\cdot)}{\longrightarrow} & \mathcal{O}_X^* & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}_D & \longrightarrow & \mathcal{O}_D & \longrightarrow & \mathcal{O}_D^* & \longrightarrow & 0 \end{array} \tag{4}$$

where $\mathbb{Z}_D \subset \mathcal{O}_D$ is the subsheaf of $\mathbb{Z}$-valued fonctions (so that $\mathbb{Z}_D \simeq \mathbb{Z}_{|D|}$) and vertical arrows are surjective restriction maps. Since X is rational, $H^i(X, \mathcal{O}_X) = 0$ for $i > 0$. Using the associated long exact cohomological sequences, we obtain the commutative diagram

$$\begin{array}{ccccccccc} & & 0 & \to & Pic(X) & \stackrel{\delta_X}{\to} & H^2(X, \mathbb{Z}_X) & \to & 0 \\ & & \downarrow & & \downarrow r & & \downarrow r' & & \downarrow \\ H^1(D, \mathbb{Z}_D) & \to & H^1(D, \mathcal{O}_D) & \stackrel{e}{\to} & Pic(D) & \stackrel{\delta_D}{\to} & H^2(D, \mathbb{Z}_D) & \to & H^2(D, \mathcal{O}_D). \end{array}$$

Here r, r' are restriction maps, δ_D, δ_X are the coboundary maps corresponding to Chern classes on D and X (see [5], Ch. 1 for the non reduced case) and e is induced by the exponential map.

We claim that r' is an isomorphism. We have the exact sequence of constant sheaves

$$0 \to j_!(\mathbb{Z}_{X_0}) \to \mathbb{Z}_X \to \mathbb{Z}_{|D|} \to 0 \tag{5}$$

where $X_0 = X \setminus |D|$ and $j : X_0 \to X$ is the inclusion, giving the exact cohomological sequence

$$H_c^2(X_0) \to H^2(X, \mathbb{Z}_X) \to H^2(|D|, \mathbb{Z}_{|D|}) \to H_c^3(X_0)$$

where $H_c^*(X_0)$ is the compact support cohomology of X_0. It is dual to the singular homology $H_*(X_0)$ of X_0 which vanishes in degree $1, 2, 3$ since $X_0 \simeq \mathbb{C}^2$, and the claim follows. Thus

$$\delta_D \circ r = r' \circ \delta_X$$

is an isomorphism, and $Pic(X)$ is a direct summand of $Pic(D)$. There remains to show that $ker(\delta_D) \simeq H^1(D, \mathcal{O}_D)$. The exponential cohomological sequence for X is exact in degree 0 so that $H^1(X, \mathbb{Z}_X) \to H^1(X, \mathcal{O}_X)$ is injective and $H^1(X, \mathbb{Z}_X) = 0$. We have just seen that $H_c^2(X_0) = 0$, and finally (5) implies $H^1(|D|, \mathbb{Z}_{|D|}) = 0$. □

Corollary 1. *There is an isomorphism $Pic(X) \simeq Pic(\partial X)$.*

Proof. By previous lemma, it's enough to show that $H^1(D_{red}, \mathcal{O}_{D_{red}}) = 0$ where $\partial X = D_{red}$ is the reduced part of D. We prove this by induction on the number of irreducible branches of D_{red}. Since $H^1(Z, \mathbb{Z}_Z) = 0$ for a finite set Z, there is a surjection

$$H^1(|D|, \mathbb{Z}_{|D|}) \to \bigoplus_{i=1}^{r} H^1(D_i, \mathbb{Z}_{D_i}).$$

Thus $H^1(D_i, \mathbb{Z}_{D_i}) = 0$ for all i and each D_i is a *rational* curve. In particular, $H^1(\mathcal{O}_{D_i}) = 0$. Moreover, $H^1_c(X_0) = 0$ so that $H^0(X, \mathbb{Z}_X) \to H^0(|D|, \mathbb{Z}_{|D|})$ is surjective and $|D|$ is connected. This shows that $|D|$ is a connected and simply connected tree of rational curves. There thus exists i so that $D_{red} = D_i + D'$, where $|D_i| \cap |D'|$ is a point and D' remains a connected and simply connected tree. The short exact sequence

$$0 \to \mathcal{O}_{D_{red}} \to \mathcal{O}_{D_i} \oplus \mathcal{O}_{D'} \to \mathcal{O}_{D_i \cdot D'} \to 0$$

gives the long exact sequence in cohomology

$$\begin{aligned} 0 \quad &\to \quad H^0(\mathcal{O}_{D_{red}}) \to H^0(\mathcal{O}_{D_i}) \oplus H^0(\mathcal{O}_{D'}) \to H^0(\mathcal{O}_{D_i \cdot D'}) \\ &\to \quad H^1(\mathcal{O}_{D_{red}}) \xrightarrow{r} H^1(\mathcal{O}_{D_i}) \oplus H^1(D', \mathcal{O}_{D'}) \to H^1(\mathcal{O}_{D_i \cdot D'}). \end{aligned}$$

By assumption, D_{red} is a *normal crossing divisor* and $D_i \cdot D' = \{pt\}$ as a *reduced* subscheme. The diagram then begins by $0 \to \mathbb{C} \to \mathbb{C} \oplus \mathbb{C} \to \mathbb{C}$, which forces r to be injective. Since $H^1(\mathcal{O}_{D_i}) = H^1(\mathcal{O}_{\{pt\}}) = 0$, this gives $H^1(\mathcal{O}_{D_{red}}) \simeq H^1(\mathcal{O}_{D'})$. □

By previous corollary, there exists an unique line bundle $\widetilde{\mathcal{L}} \in Pic(X)$ so that $\widetilde{\mathcal{L}}_{|\partial X} \simeq \mathcal{L}_{|\partial X}$ and $\mathcal{L}$ lifts to X if and only if

$$\mathcal{L}_0 := \mathcal{L} \otimes \widetilde{\mathcal{L}}^{-1}_{|D} \simeq \mathcal{O}_D.$$

Since $\delta_D(\mathcal{L}_0) = 0$ (by construction), there exists $\beta \in H^1(D, \mathcal{O}_D)$ with $e(\beta) = \mathcal{L}_0$. Moreover e is injective and

$$\mathcal{L}_0 \simeq \mathcal{O}_D \iff \beta = 0.$$

There remains to make explicit such a condition. We first use Cech cohomology. Suppose that $\mathcal{L}_0$ is given by the one cocycle class $g = \{g_{UV}\} \in H^1(D, \mathcal{O}_D^*)$, relative to some open covering $\mathcal{U}$ of X. We can suppose $\mathcal{U}$ fine enough to ensure a logarithmic determination

$$\widetilde{h}_{UV} := \frac{1}{2i\pi} log(\widetilde{g}_{UV}) \in \mathcal{O}_X(U \cap V),$$

where $\widetilde{g}_{UV} \in \mathcal{O}_X^*(U \cap V)$ is some local lifting of g_{UV}. Since $\delta_D(g) = 0$, the classes $h_{UV} \in \mathcal{O}_D(U \cap V)$ define a 1-cocycle class $\{h_{UV}\} \in H^1(D, \mathcal{O}_D)$ which represents β (this definition does not depend on the liftings). Since X is rational, the structural sequence for D

$$0 \longrightarrow \mathcal{O}_X(-D) \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{O}_D \longrightarrow 0$$

gives rise to a coboundary *isomorphism* $\delta : H^1(D, \mathcal{O}_D) \to H^2(X, \mathcal{O}_X(-D))$. Serre Duality gives a non degenerate pairing

$$H^2(X, \mathcal{O}_X(-D)) \otimes H^0(X, \Omega^2_X(D)) \xrightarrow{(\cdot,\cdot)} H^2(X, \Omega^2_X) \overset{Tr}{\simeq} \mathbb{C}$$

where Tr is the trace map [5]. We identify $\mathcal{O}_X(-D)$ with the sheaf of functions vanishing on D and $\Omega^2_X(D)$ with the sheaf of meromorphic 2-forms with polar locus

bounded by D. The Serre pairing $(\delta(\beta), \Psi)$ with $\Psi \in H^0(X, \Omega^2_X(D))$ is represented by the 2-cocyle class

$$\zeta_\Psi := \left\{ (\widetilde{h}_{UV} + \widetilde{h}_{VW} + \widetilde{h}_{WU})\Psi_{|U\cap V\cap W} \right\} \in H^2(X, \Omega^2_X)$$

and $\beta = 0$ if and only if

$$Tr(\zeta_\Psi) = 0 \quad \forall\ \Psi \in H^0(X, \Omega^2_X(D)).$$

To make explicit the complex numbers $Tr(\zeta_\Psi)$, we use the Dolbeault $\bar\partial$-resolution of Ω^2_X. We denote by $\mathcal{D}^{(p,q)}_X$ the sheaf of germs of (p,q)-currents on X. Let ψ be a germ of meromorphic q-form at $p \in X$. We recall for convenience that the *principal value* current $[\psi] \in \mathcal{D}^{(q,0)}_{X,p}$ and the *residue current* $\bar\partial[\psi] \in \mathcal{D}^{(q,1)}_{X,p}$ have the Cauchy integral representations

$$\langle [\psi], \theta\rangle := \lim_{\epsilon\to 0} \frac{1}{2i\pi} \int_{U\cap\{|u|>\epsilon\}} \psi \wedge \theta$$

and

$$\langle \bar\partial[\psi], \theta\rangle := \lim_{\epsilon\to 0} \frac{1}{2i\pi} \int_{U\cap\{|u|=\epsilon\}} \psi \wedge \theta,$$

where θ is some form-test with appropriate bidegree and $u = 0$ is a local equation for the polar divisor of ψ in a small neighborhood U of p (see [30] for instance). The Dolbeault resolution of Ω^2_X is given by the exact complex of sheaves

$$0 \longrightarrow \Omega^2_X \xrightarrow{[\cdot]} \mathcal{D}^{(2,0)}_X \xrightarrow{\bar\partial} \mathcal{D}^{(2,1)}_X \xrightarrow{\bar\partial} \mathcal{D}^{(2,2)}_X \longrightarrow 0.$$

This sequence breaks in the two short exact sequences

$$0 \to \Omega^2_X \to \mathcal{D}^{(2,0)}_X \xrightarrow{\bar\partial} \mathcal{Z}^{(2,1)}_X \to 0 \quad \text{and} \quad 0 \to \mathcal{Z}^{(2,1)}_X \to \mathcal{D}^{(2,1)}_X \xrightarrow{\bar\partial} \mathcal{D}^{(2,2)}_X \to 0,$$

where $\mathcal{Z}^{(2,1)}_X \subset \mathcal{D}^{(2,1)}_X$ is the subsheaf of $\bar\partial$-closed $(2,1)$-currents. Since the sheaves $\mathcal{D}^{(p,q)}_X$ are fine, we obtain the two coboundary *isomorphisms*

$$\frac{H^0(X, \mathcal{D}^{(2,2)}_X)}{\bar\partial H^0(X, \mathcal{D}^{(2,1)}_X)} \xrightarrow{\delta_1} H^1(X, \mathcal{Z}^{(2,1)}_X) \quad \text{and} \quad H^1(X, \mathcal{Z}^{(2,1)}_X) \xrightarrow{\delta_2} H^2(X, \Omega^2_X).$$

Thus, for any Ψ, there exists a global $(2,2)$-current $T_\Psi \in H^0(X, \mathcal{D}^{(2,2)}_X)$ whose class $[T_\Psi]$ modulo $\bar\partial$ is unique solution to $\zeta_\Psi = \delta_2 \circ \delta_1([T_\Psi])$, and we have equality

$$Tr(\zeta_\Psi) = \langle T_\Psi, 1\rangle.$$

To make explicit T_Ψ, we need the following lemma.

Lemma 2. *1. There exists an open tubular neighborhood B of $|D|$ and a Cartier divisor $\widetilde{\gamma}$ on B which restricts to γ on D.*

2. There exists is isomorphism $\widetilde{\mathcal{L}} \simeq \mathcal{O}_X(E)$ for a Cartier divisor E which restricts to Γ on D_{red}.

Proof. 1. By mean of partition of unity, we can construct u a $\mathcal{C}^\infty$ function on X which vanishes exactly on $|D|$, giving an open tubular neighborhood of D

$$B_\epsilon = \{|u| < \epsilon\}.$$

Let $f = \{f_U\}$ be a meromorphic section of $\mathcal{L}$ with Cartier divisor γ, and consider some local liftings $\widetilde{f}_U \in \mathcal{M}_X(U)$, with $\mathcal{M}_X$ the sheaf of meromorphic functions on B. We can choose $\mathcal{V}$ a sufficiently fine covering of B_ϵ in order to suppose that

$U \cap V \cap |\Gamma| = \emptyset$ for distinct $U, V \in \mathcal{V}$, with moreover $\widetilde{f}_U \in \mathcal{O}_X(U)^*$ for $U \cap |\Gamma| = \emptyset$. If now U intersects $|\Gamma|$, we can choose $\epsilon' < \epsilon$ small enough so that $\widetilde{f}_U \in \mathcal{M}_X(U)$ has nor poles nor zeroes on $U \cap V \cap B_{\epsilon'}$. In such a way, $\widetilde{f}_U/\widetilde{f}_V$ is invertible on $U \cap V \cap B_{\epsilon'}$, giving a Cartier divisor $\widetilde{\gamma}$ on $B_{\epsilon'}$ which restricts to γ on D.

2. Let $\mathcal{F} = \mathcal{O}_X(F)$ be some very ample line bundle on X with F an effective divisor which intersects properly $|D_{red}|$. The isomorphisms

$$\mathcal{O}_{D_{red}}(\Gamma) \simeq \mathcal{L}_{|D_{red}} \simeq \widetilde{\mathcal{L}}_{|D_{red}}$$

combined with the structural sequence for D_{red} gives the exact sequence

$$0 \to \widetilde{\mathcal{L}} \otimes \mathcal{O}_X(nF - D_{red}) \to \widetilde{\mathcal{L}} \otimes \mathcal{O}_X(nF) \to \mathcal{O}_{D_{red}}(\Gamma + n\Gamma_F) \to 0$$

for any integer n, where $\Gamma_F = F \cdot D_{red}$. For n big enough, we have

$$H^1(\widetilde{\mathcal{L}} \otimes \mathcal{O}_X(nF - D_{red})) = 0$$

by Serre Vanishing Theorem so that $\Gamma + n\Gamma_F$ lifts to some Cartier divisor G on X. Then, the Cartier divisor $E = G - nF$ restricts to Γ on D_{red}. By construction $\mathcal{O}_X(E)$ and $\mathcal{L} = \mathcal{O}_D(\gamma)$ have the same restriction to $\partial X = D_{red}$, and Corollary 2 implies $\widetilde{\mathcal{L}} \simeq \mathcal{O}_X(E)$. □

Let $B, \widetilde{\gamma}$ and E as in Lemma 2, with $\mathcal{V}$ the associated open covering of B. Since $\mathcal{O}_B(\widetilde{\gamma}) \otimes \mathcal{O}_B(-E)$ restricts to $\mathcal{L}_0$ on D, we can choose the liftings $\widetilde{g}_{UV} = m_U/m_V$, where $m = \{m_U\}_{U \in \mathcal{V}}$ is the global meromorphic section of $\mathcal{O}_B(\widetilde{\gamma}) \otimes \mathcal{O}_B(-E)$ with Cartier divisor

$$div(m) = \widetilde{\gamma} - E_{|B}$$

on B. By construction, $m_{U|U\cap V} \in \mathcal{O}_B^*(U \cap V)$ for distinct $U, V \in \mathcal{V}$. Thus, there exists a logarithmic determination

$$log(m_{U|U\cap V}) := \sum_{n=1}^{\infty} \frac{1}{n}\big((1 - m_{U|U\cap V})\big)^n$$

of $m_{U|U\cap V}$. Since $div(m) \cdot D_{red} = 0$, the restriction of m to D_{red} is a constant, that we can suppose to be 1. There thus exists $n_0 \in \mathbb{N}$ such that the meromorphic function $(1 - m_U)^n$ vanishes on the divisor $D \cap U$ for all $n \geq n_0$ and all $U \in \mathcal{V}$.

Let $\Psi \in H^0(X, \Omega_X^2(D))$. By the Duality Theorem [30], we have

$$\big[\big(1 - m_U\big)^n\big]\bar{\partial}\big[\Psi_U\big] = 0 \quad \forall\, n \geq n_0$$

so that the principal value currents

$$S_U := \sum_{n=1}^{n_0} \frac{1}{n}\Big[\big(1 - m_U\big)^n\Big]$$

satisfy

$$(S_U - S_V)\bar{\partial}\big[\Psi_{U\cap V}\big] = \big[log(\widetilde{g}_{U\cap V})\big]\bar{\partial}\big[\Psi_{U\cap V}\big] \tag{6}$$

for all $U, V \in \mathcal{V}$. We obtain in such a way a global $(2,2)$-current $T_B \in \Gamma(B, \mathcal{D}_B^{(2,2)})$ on B, locally given by

$$T_U = \bar{\partial} S_U \wedge \bar{\partial}[\Psi_U]$$

for all $U \in \mathcal{V}$. Since $\bar{\partial}[\Psi_U] = 0$ for all U with $U \cap |D| = \emptyset$, we can extend T_B by zero to a global current T on X. Using (6) and the definition of the coboundary maps, it's now straightforward to check that T is solution to

$$\delta_2 \circ \delta_1(T) = \zeta_\Psi.$$

Let now ψ be some rational 1-form on X so that $d\psi_{|X_0} = \Psi_{|X_0}$. For all $U \in \mathcal{V}$, we define the local currents

$$R_U := \Big(dS_U - \Big[\frac{dm_U}{m_U}\Big]\Big) \wedge \bar\partial\big[\psi_U\big] \quad \text{and} \quad T'_U = \bar\partial\Big[\frac{dm_U}{m_U}\Big] \wedge \bar\partial\big[\psi_U\big].$$

From (6) we deduce equalities $R_{U|U\cap V} = R_{V|U\cap V}$, and the R_U's define a global $(2,1)$-current R_B on B. By assumption, m_U/m_V is invertible on $U \cap V$ so that $T'_{U|U\cap V} = T'_{V|U\cap V}$, giving a global $(2,2)$-current T'_B on B. Both currents are supported on $|D| \subset B$ and can be extended by zero to global currents R and T' on X.

Since T_U has support a finite set, Stokes Theorem gives equalities

$$\begin{aligned}\langle T_U, 1\rangle &= \langle \bar\partial S_U \wedge \bar\partial[\Psi_U], 1\rangle \\ &= \langle \bar\partial S_U \wedge \bar\partial d[\psi_U], 1\rangle \\ &= \langle \bar\partial(dS_U) \wedge \bar\partial[\psi_U], 1\rangle = \langle T'_U + \bar\partial R_U, 1\rangle.\end{aligned}$$

Thus, $\langle T, 1\rangle = \langle T' + \bar\partial R, 1\rangle = \langle T', 1\rangle$. Since $div(m) = \widetilde{\gamma} - E_{|B}$ on B, the Lelong-Poincaré equation gives equality

$$\langle T', 1\rangle = \langle T'_B, 1\rangle = \langle [\widetilde{\gamma}] \wedge \bar\partial[\psi]_{|B}, 1\rangle - \langle [E]_{|B} \wedge \bar\partial[\psi]_{|B}, 1\rangle,$$

where $[\cdot]$ designs here the integration current associated to analytic cycles. The current $[E]_{|B} \wedge \bar\partial[\psi]_{|B}$ is supported on the compact subset $|\Gamma| \subset B$, and the integration current is $\bar\partial$-closed. We deduce

$$\langle [E]_{|B} \wedge \bar\partial[\psi]_{|B}, 1\rangle = \langle [E] \wedge \bar\partial[\psi], 1\rangle = \langle \bar\partial([E] \wedge [\psi]), 1\rangle = 0.$$

This is also equivalent to the Residue Theorem [20]. For B small enough, $B \cap \widetilde{\gamma}$ is a disjoint union of analytic cycles $\widetilde{\gamma}_p = \{f_p = 0\}$. If ψ_p is the germ of ψ at p in the chosen local coordinates, we obtain finally

$$\begin{aligned}Tr(\zeta_\Psi) &= \sum_{p\in|\Gamma|} \langle [\widetilde{\gamma}_p] \wedge \bar\partial[\psi_p], 1\rangle \\ &= \sum_{p\in|\Gamma|} res_p\big(\frac{df_p}{f_p} \wedge \psi_p\big) = \sum_{p\in|\Gamma|} \langle \gamma, \Psi\rangle_p.\end{aligned}$$

This expression only depends on $\mathcal{O}_D(\gamma)$ and Ψ by construction.

Conditions (2) of Theorem 2 are thus equivalent to that $\mathcal{L} = \mathcal{O}_D(\gamma)$ extends to $\widetilde{\mathcal{L}} \in Pic(X)$. If $\mathcal{L}$ extends to $\widetilde{\mathcal{L}}$, we can use Vanishing Serre Theorem as in Lemma 2 (with (D,γ) instead of (D_{red},Γ)) and show that $\widetilde{\mathcal{L}} \simeq \mathcal{O}_X(E)$ for some Cartier divisor E on X which restricts to γ on D. The lifting bundle $\widetilde{\mathcal{L}}$ being unique (up to isomorphism), the osculating divisor E is unique up to rational equivalence. This ends the proof of the first point.

If conditions (2) hold, then $\mathcal{L} \simeq \mathcal{O}_D(E)$ for some Cartier divisor E on X. By tensoring the structural sequence of D with $\widetilde{\mathcal{L}} = \mathcal{O}_X(E)$, we obtain the short exact sequence

$$0 \to \mathcal{O}_X(E-D) \to \mathcal{O}_X(E) \to \mathcal{O}_D(E) \to 0.$$

If γ is effectif and $H^1(X, \mathcal{O}_X(E-D)) = 0$, the global section $f \in H^0(D, \mathcal{O}_D(E))$ with zero divisor γ automatically lifts to $\widetilde{f} \in H^0(X, \mathcal{O}_X(E))$ and $C := div_0(\widetilde{f})$ is an *effective* osculating divisor for (D,γ). This ends the proof of Theorem 1. □

2.5. **An explicit formula in the toric case.** We show now that we can make explicit the conditions (2) in the case of a toric variety X. We refer the reader to [14] and [11] for an introduction to toric geometry.

2.5.1. *Preleminaries.* Suppose that X is a *toric* surface containing X_0 as an union of open orbits. Then, X has toric divisors $D_0, \dots, D_{r+1}$ where

$$\partial X = D_1 + \cdots + D_r$$

is the boundary of X and D_0 and D_{r+1} are the Zariski closure of the one dimensional open orbits of $X_0 \simeq \mathbb{C}^2$.

Let Σ be the fan of X. We denote by $\rho_i \in \Sigma$ the ray associated to the toric divisor D_i. Since Σ is regular, we can order the D_i's in such a way that the generators η_i of the monoids $\rho_i \cap \mathbb{Z}^2$ satisfy

$$det(\eta_i, \eta_{i+1}) = 1$$

(with convention $\eta_{r+2} = \eta_0$).

We denote by U_i the affine toric chart associated to the two-dimensional cone $\rho_i\mathbb{R}^+ \oplus \rho_{i+1}\mathbb{R}^+$. Thus,

$$U_i = Spec\, \mathbb{C}[x_i, y_i] \simeq \mathbb{C}^2,$$

where torus coordinates $t = (t_1, t_2)$ and affine coordinates (x_i, y_i) are related by relations

$$t^m = x_i^{\langle m, \eta_i \rangle} y_i^{\langle m, \eta_{i+1} \rangle}$$

for all $m = (m_1, m_2) \in \mathbb{Z}^2$, where $t^m = t_1^{m_1} t_2^{m_2}$ (see [11]). With these conventions, the toric divisors D_i and D_{i+1} have respective affine equations

$$D_{i|U_i} = \{x_i = 0\} \quad \text{and} \quad D_{i+1|U_i} = \{y_i = 0\}$$

and $|D_j| \cap U_i = \emptyset$ for $j \neq i, i+1$.

We can associate to any toric divisor $E = \sum_{i=0}^{r+1} e_i D_i$ a polytope

$$P_E = \{m \in \mathbb{R}^2, \langle m, \eta_i \rangle + e_i \geq 0,\ i = 0, \dots, r+1\},$$

where $\langle \cdot, \cdot \rangle$ designs the usual scalar product in $\mathbb{R}^2$. Each Laurent monomial t^m defines a rational function on X with divisor

$$div(t^m) = \sum_{i=0}^{r+1} \langle m, \eta_i \rangle D_i$$

and there is a natural isomorphism

$$H^0(X, \mathcal{O}_X(E)) \simeq \bigoplus_{m \in P_E \cap \mathbb{Z}^2} \mathbb{C} \cdot t^m, \tag{7}$$

where $H^0(X, \mathcal{O}_X(E))$ is the vector space of rational functions $h \in \mathbb{C}(X)$ for which $div(h) + E \geq 0$. Finally, we recall that the toric divisor

$$-K_X := D_0 + \cdots + D_{r+1}$$

is an anticanonical divisor for X.

2.5.2. *Explicit osculating criterions.* Let (D,γ) be an osculation data on ∂X. We note $\Gamma = \gamma\cdot\partial X$ and $\Gamma_i = \gamma\cdot D_i$. We assume that the following hypothesis holds:

(H_1) *The zero-cycle* Γ *is reduced and does not contain any torus fixed points.*

Thus, the germs $\widetilde{\gamma}_p$ are smooth, irreducible, and have transversal intersection with ∂X. For each $p\in|\Gamma|$, there is an unique component D_i containing p and we can choose the Weiertrass equation

$$f_p(x_i,y_i) = y_i - \phi_p(x_i)$$

for the associated germ $\widetilde{\gamma}_p$. The analytic function $\phi_p\in\mathbb{C}\{x_i\}$ is well-defined modulo $(x_i^{k_i+1})$ and does not vanish at 0. We obtain the following

Corollary 2. *With previous hypothesis and notations, conditions* (2) *become*

$$\sum_{i\in I_m^-}\frac{1}{(-\langle m,\eta_i\rangle)!}\left[\frac{\partial^{-\langle m,\eta_i\rangle}}{\partial x_i^{-\langle m,\eta_i\rangle}}\left(\sum_{p\in|\Gamma_i|}\frac{\phi_p^{\langle m,\eta_{i+1}\rangle}}{\langle m,\eta_{i+1}\rangle}\right)\right](0)=0 \tag{8}$$

for all $m\in P_{D+K_X}\cap\mathbb{Z}^2$, *where*

$$I_m^- = \{i\in\{1,\dots,r\},\ \langle m,\eta_i\rangle\le 0\},$$

and with convention $\phi_p^k/k := log(\phi_p)$ *for* $k=0$.

The previous expression is well-defined, being a rational expression on the successive derivatives and logarithmic derivatives of the ϕ_p's evaluated at 0 (recall that $\phi_p(0)\neq 0$). Note that we don't exclude that $\Gamma_i=0$ for some i.

Example 2 (Wood's theorem). We keep the same hypothesis and notations of Example 1, with now an osculating order $k\ge 2$. Thus $D=(k+1)L$. Hypothesis (H_1) holds and by Corollary 1, there exists an osculating divisor for (D,γ) if and only if

$$\frac{\partial^{m_1+m_2}}{\partial x^{m_1+m_2}}\Big(\sum_{p\in|\Gamma|}\frac{\phi_p^{m_1}}{m_1}\Big)(0)=0,\quad\forall\, m\in(\mathbb{N}^*)^2,\ m_1+m_2\le k. \tag{9}$$

Note that $H^1(\mathcal{O}_{\mathbb{P}^2}(d-k-1))=0$ if $k\le d+1$. In such a case, (9) is also sufficient for the existence of an osculating algebraic *curve*. We recover here a theorem of Wood, [34].

2.5.3. *Proof of Corollary 2.* For $m\in\mathbb{Z}^2$, we denote by Ψ_m the rational form given by

$$\Psi_{m|(\mathbb{C}^*)^2} = t^m\frac{dt_1\wedge dt_2}{t_1t_2}$$

in torus coordinates. Then, $div(\Psi_m) = div(t^m) - K_X$ and there is equality

$$H^0(X,\Omega_X^2(D)) = \bigoplus_{m\in P_{D+K_X}\cap\mathbb{Z}^2}\mathbb{C}\ \cdot\ \Psi_m.$$

Let $m\in P_{D+K_X}$. In particular $\langle m,\eta_0\rangle\ge 1$ and we can suppose that $m_2\neq 0$. The form Ψ_m is holomorphic in X_0 and $\Psi_{m|X_0} = d(\psi_{m|X_0})$ where ψ_m is the rational

1-form on X determined by its restriction

$$\psi_{m|(\mathbb{C}^*)^2} = \frac{t^m}{m_2}\frac{dt_1}{t_1}$$

to the torus. Let $p \in |\Gamma_i|$. We compute the associated residue in the chart U_i. If we let (e_1, e_2) be the canonical basis of $\mathbb{R}^2$, we obtain

$$\psi_{m|U_i} = x_i^{\langle m,\eta_i\rangle} y_i^{\langle m,\eta_{i+1}\rangle} \frac{1}{m_2}\big[\langle e_1,\eta_i\rangle\frac{dx_i}{x_i} + \langle e_1,\eta_{i+1}\rangle\frac{dy_i}{y_i}\big].$$

If $\langle m,\eta_i\rangle > 0$, the form ψ_m is holomorphic at $p \in |\Gamma_i|$ and $res_p(\frac{df_p}{f_p}\wedge\psi_m) = 0$. Suppose now that $\langle m,\eta_i\rangle \leq 0$. The Cauchy integral representation for Grothendieck residues of meromorphic forms does not depend on $\underline{\epsilon}$ for ϵ_i small enough, thanks to Stokes Theorem. Thus, for sufficiently small ϵ_i's, we obtain

$$\begin{aligned}
& res_p\Big[x_i^{\langle m,\eta_i\rangle} y_i^{\langle m,\eta_{i+1}\rangle}\frac{df_p}{f_p}\wedge\frac{dy_i}{y_i}\Big] \\
= & -\frac{1}{(2i\pi)^2}\int_{|x_i|=\epsilon_1,|y_i-\phi_p|=\epsilon_2} x_i^{\langle m,\eta_i\rangle} y_i^{\langle m,\eta_{i+1}\rangle}\frac{d\phi_p}{y_i-\phi_p}\wedge\frac{dy_i}{y_i} \\
= & \frac{1}{(2i\pi)^2}\int_{|x_i|=\epsilon_1}\left(\int_{|y_i-\phi_p|=\epsilon_2} y_i^{\langle m,\eta_{i+1}\rangle-1}\frac{dy_i}{y_i-\phi_p}\right)x_i^{\langle m,\eta_i\rangle}d\phi_p \\
= & \frac{1}{2i\pi}\int_{|x_i|=\epsilon} x_i^{\langle m,\eta_i\rangle}\phi_p^{\langle m,\eta_{i+1}\rangle-1}\phi_p' dx \\
= & \frac{1}{(-\langle m,\eta_i\rangle-1)!}\left[\frac{\partial^{-\langle m,\eta_i\rangle}}{\partial x_i^{-\langle m,\eta_i\rangle}}\left(\frac{\phi_p^{\langle m,\eta_{i+1}\rangle}}{\langle m,\eta_{i+1}\rangle}\right)\right]_{x_i=0}
\end{aligned}$$

where the two last equalities are application of the Cauchy formula. If $\langle m,\eta_{i+1}\rangle = 0$,

$$\frac{\phi_p^{\langle m,\eta_{i+1}\rangle}}{\langle m,\eta_{i+1}\rangle} := log(\phi_p)$$

is only defined up to some constant (recall that $\phi_p(0)\neq 0$) but $0 \notin P_{D+K_X}$ so that $\langle m,\eta_i\rangle > 0$ in that case. Thus previous expression only depends on the logarithmic derivatives of ϕ_p, so is well-defined. In the same way, but simpler, we find

$$res_p\Big[x_i^{\langle m,\eta_i\rangle} y_i^{\langle m,\eta_{i+1}\rangle}\frac{df_p}{f_p}\wedge\frac{dx_i}{x_i}\Big] = \frac{-1}{(-\langle m,\eta_i\rangle)!}\left[\frac{\partial^{-\langle m,\eta_i\rangle}}{\partial x_i^{-\langle m,\eta_i\rangle}}\big(\phi_p^{\langle m,\eta_{i+1}\rangle}\big)\right]_{x_i=0},$$

the minus sign coming from the chosen ordering of the numerator's factors. We deduce

$$res_p\Big(\frac{df_p}{f_p}\wedge\psi_m\Big) = \frac{C}{m_2}\times\frac{1}{(-\langle m,\eta_i\rangle)!}\left[\frac{\partial^{-\langle m,\eta_i\rangle}}{\partial x_i^{-\langle m,\eta_i\rangle}}\left(\frac{\phi_p^{\langle m,\eta_{i+1}\rangle}}{\langle m,\eta_{i+1}\rangle}\right)\right]_{x_i=0}$$

where

$$C = \langle e_1,\eta_i\rangle\langle m,\eta_{i+1}\rangle - \langle e_1,\eta_{i+1}\rangle\langle m,\eta_i\rangle = m_2 det(\eta_i,\eta_{i+1}) = m_2.$$

This ends the proof of Corollary 1. □

If two algebraic curves of fixed degree osculate each other on a finite subset with sufficiently big contact orders, they necessarily have a common component.

We show in the next section that this basic fact permits to apply Theorem 1 and Corollary 1 to the Computer Algebra problem of polynomial factorization.

3. Application to polynomial factorization.

This section is devoted to develop a new algorithm to compute the absolute factorization of a bivariate polynomial f. The method we introduce uses vanishing-sums in the vain of the Galligo-Rupprecht algorithm [13]. The main difference is that the underlying algorithmic complexity depends now on the Newton polytope N_f instead of the usual degree $d = deg(f)$. Our algorithm is comparable to a toric version of the Hensel lifting, in the spirit of the Abu Salem-Gao-Lauder algorithm [1]. We prove our main results Theorem 2 and Proposition 1 in Subsections 3.2 and 3.3. We describe a sketch of algorithm in Subsection 3.4 and we comment and compare it with related results in Subsection 3.5. We discuss non toric singularities in Subsection 3.6 and we conclude in the last Subsection 3.7.

3.1. **Preliminaries and notations.** Let $f \in K[t_1, t_2]$ be a bivariate polynomial with coefficients in some subfield $K \subset \mathbb{C}$. By absolute factorization of f, we mean its irreducible decomposition in the ring $\mathbb{C}[t_1, t_2]$, computed with floatting numbers with a given precision.

Suppose that f has the monomial expansion

$$f(t) = \sum_{m \in \mathbb{N}^2} c_m t^m,$$

with the usual notations $m = (m_1, m_2) \in \mathbb{Z}^2$ and $t^m = t_1^{m_1} t_2^{m_2}$. We denote by N_f the Newton polytope of f, convex hull of the exponents $m \in \mathbb{N}^2$ for which $c_m \neq 0$. We recall that by a theorem of Ostrovski [28], we have relations

$$N_{f_1 f_2} = N_{f_1} + N_{f_2}$$

for any polynomials f_1, f_2, where $+$ designs here the Minkowski sum.

We definitively assume that the following hypothesis holds.

(H_2) *The Newton polytope of f contains the origin.*

This equivalent to that $f(0, 0) \neq 0$. An *exterior facet* of N_f is a one-dimensional face F of N_f whose normal inward primitive vector has non simultaneously positive coordinates. The associated normal ray of N_f is called an *exterior ray*. The associated exterior facet polynomial f_F of f is defined to be

$$f_F = \sum_{m \in F \cap \mathbb{Z}^2} c_m t^m.$$

The facet polynomials have a one dimensional Newton polytope and become univariate polynomials after a monomial change of coordinates.

We construct now a toric completion of $\mathbb{C}^2$ associated to the exterior facets of N_f. To this aim, we consider the *complete* simplicial fan Σ_f of $\mathbb{R}^2$ whose rays are

$$\Sigma_f(1) = \{exterior\ rays\ of\ N_f\} \cup \{(0, 1)\mathbb{R}^+, (1, 0)\mathbb{R}^+\}.$$

The toric surface $X_f = X_{\Sigma_f}$ is a simplicial toric completion of $\mathbb{C}^2 = Spec\, \mathbb{C}[t_1, t_2]$ whose boundary $\partial X_f = X_f \backslash \mathbb{C}^2$ is the sum of the irreducible toric divisors associated to the exterior rays of N_f.

By hypothesis (H_2), the fan Σ_f refines the normal fan of N_f. The intersection of the Zariski closure $C_f \subset X_f$ of the affine curve $\{f=0\} \subset \mathbb{C}^2$ with the irreducible components of the boundary ∂X_f corresponds to the *non trivial* roots of the exterior facet polynomial of f (see [24] for instance). In particular, the curve C_f does not contain any torus fixed points. We say that f satisfies hypothesis (H_1) of Subsection 2.5 when the zero-cycle $\Gamma_f = C_f \cdot \partial X_f$ does. This corresponds to the case of exterior facet polynomials of f with a square free absolute decomposition in $\mathbb{C}[t,t^{-1}]$.

The boundary of X_f contains the singular locus $S := Sing(X_f)$ of X_f and is generally not a normal crossing divisor. To this aim, we consider a toric desingularization

$$X \xrightarrow{\pi} X_f$$

of X_f, whose exceptional divisor E satisfies $S = \pi(|E|)$. The smooth surface X is now a projective toric $\mathbb{C}^2$-completion with a toric normal crossing boundary

$$\partial X = D_1 + \cdots + D_r$$

whose support contains $|E|$. Since $C_f \cap S = \emptyset$, the total transform $C = \pi^{-1}(C_f)$ of C_f has a proper intersection with ∂X and the irreducible decomposition of C corresponds to the absolute factorization of f. Note that C is not necessarily reduced.

As in Subsection 2.5, we denote by $\rho_0, \ldots, \rho_{r+1}$ the rays of the fan Σ of X, and by $\eta_0, \ldots, \eta_{r+1}$ their primitive vectors. So $\eta_0 = (0,1)$ and $\eta_{r+1} = (1,0)$. The curve C has a positive intersection $C \cdot D_i > 0$ when $\rho_i \in \Sigma(1)$ is an exterior ray of N_f, and $C \cdot D_i = 0$ when $\rho_i \in \Sigma(1) \setminus \Sigma_f(1)$ (that is when $\pi(|D_i|) \subset S$).

We'll need the following lemma

Lemma 3. *There is an unique effective divisor D linearly equivalent to $C + \partial X$ with support $|\partial X|$. Moreover, the following equality*

$$P_{D+K_X} \cap \mathbb{Z}^2 = N_f \cap (\mathbb{N}^*)^2$$

holds.

Proof. The polynomial f extends to a rational function on X whose polar divisor $div_\infty(f)$ is supported by $|\partial X|$. Thus, the divisor

$$D := div_\infty(f) + \partial X$$

is effective, with support $|\partial X|$, and rationally equivalent to $C + \partial X$. If D' is an other candidate, then $D - D' = div(h)$ for some $h \in \mathbb{C}(X)$ with no poles nor zeroes outside $|\partial X|$. Since $X \setminus |\partial X| \simeq \mathbb{C}^2$, the rational function h is necessarily constant and $D = D'$.

Let us note $G := div_\infty(f)$ and P_G its associated polytope. By (7), N_f is contained in P_G with at least one point on each face of P_G. Since the fan of X refines the nornal fan of f, both polytopes have parallelic facets and it follows that $P_G = N_f$. Now, $D + K_X = G + K_X + \partial X = G - D_0 - D_{r+1}$ so that

$$P_{D+K_X} = \{m \in P_G,\ \langle m, \eta_0 \rangle \geq 1,\ \langle m, \eta_{r+1} \rangle \geq 1\}.$$

We finally obtain equality $P_{D+K_X} \cap \mathbb{Z}^2 = N_f \cap (\mathbb{N}^*)^2$. □

3.2. **Computing the Newton polytopes of the absolute factors.** We show here how to recover the Newton polytopes of the irreducible absolute factors of N_f.

We recall that the Newton polytope of a factor of f is necessarily a Minkowski summand of N_f. For a general polytope Q, we denote by $Q^{(i)}$ the set of $m \in Q$ for which the scalar product $\langle m, \eta_i \rangle$ is minimal.

We obtain the following

Theorem 2. *1. Let $f \in K[t_1, t_2]$ which satisfies (H_2). Let π, X and C be as before and denote by γ the restriction of C to the divisor D of Lemma 3. Let Q be a lattice Minkowski summand of N_f.*

There exists an absolute factor q of f with Newton polytope Q if and only if there exists $\gamma' \leq \gamma$ an effective Cartier divisor on D with

$$deg(\gamma' \cdot D_i) = Card(Q^{(i)} \cap \mathbb{Z}^2) - 1, \ i = 1, \dots, r \tag{10}$$

and such that (2) holds for the osculation data (D, γ') on the boundary of X. These conditions are independant of the choice of π. The polynomial q can be recovered from γ'.

Proof. A Minkowski sum decomposition $N_f = P + Q$ corresponds to a line bundle decompostion

$$\mathcal{O}_X(G) = \mathcal{O}_X(G_P) \otimes \mathcal{O}_X(G_Q),$$

where G, G_P and G_Q are the polar divisors of the rational functions determined by polynomials with respective polytope N_f, P and Q. Note that $G = G_P + G_Q$. Since Σ refines the normal fan of each polytope, we have equalities $N_f = P_G$, $Q = P_{G_Q}$ and $P = P_{G_P}$ (see Lemma 3) and all involved line bundles are globally generated over X (see [14]).

A factor of f with Newton polytope Q corresponds to a divisor $C' \leq C$ lying in the complete linear system $|\mathcal{O}_X(G_Q)|$. It defines a Cartier divisor $\gamma' = C'_{|D} \leq C_{|D} = \gamma$ on D. Thus, conditions (2) hold for the osculation data (D, γ') and

$$deg(\gamma' \cdot D_i) = deg(C' \cdot D_i) = deg(\mathcal{O}_X(G_Q)_{|D_i})$$

for all $i = 1, \dots, r$. Since $\mathcal{O}_X(G_Q)$ is globally generated over X, toric intersection theory gives equalities

$$deg(\mathcal{O}_X(G_Q)_{|D_i}) = Card(Q^{(i)} \cap \mathbb{Z}^2) - 1$$

for all $i = 1, \dots, r$. This shows necessity of conditions. Note that $i \in I_\pi$ implies $C' \cdot D_i = 0$ in which case $Q^{(i)}$ is reduced to a point.

Suppose now that (D, γ') satisfies (10) and (2) and let F be an osculating divisor asociated to that data. We deduce equalities

$$deg\, \mathcal{O}_X(F)_{|D_i} = deg(\gamma' \cdot D_i) = deg\, \mathcal{O}_X(G_Q)_{|D_i}$$

for all $i = 1, \dots, r$. Thus, there is an isomorphism

$$\mathcal{O}_{\partial X}(F) \simeq \mathcal{O}_{\partial X}(G_Q)$$

and $\mathcal{O}_X(F) \simeq \mathcal{O}_X(G_Q)$ by Corollary 1 of Subsection 2.4. Finally, (2) and (10) hold for (D, γ') if and only if

$$\mathcal{O}_D(\gamma') \simeq \mathcal{O}_D(G_Q).$$

Let us show that there exists in such a case an *effective* osculating divisor. The problem is that $H^1(X, \mathcal{O}_X(G_Q - D))$ does not necessarily vanish. To avoid this difficulty, we introduce the effective divisor

$$D_Q := G_Q + \partial X \leq G + \partial X = D.$$

Then $\mathcal{O}_{D_Q}(G_Q) \simeq \mathcal{O}_{D_Q}(\gamma'_{|D_Q})$ and

$$H^1(X, \mathcal{O}_X(G_Q - D_Q)) \simeq H^1(X, \mathcal{O}_X(-\partial X)).$$

Since ∂X is reduced and connected, the restriction map $H^0(\mathcal{O}_X) \to H^0(\mathcal{O}_{\partial X})$ is an isomorphism and we deduce equality $H^1(X, \mathcal{O}_X(-\partial X)) = 0$. By Theorem 1, there thus exists $C' \in |\mathcal{O}_X(G_Q)|$ with

$$C'_{|D_Q} = \gamma'_{|D_Q}.$$

Such a curve has a proper intersection with the remaining toric divisors D_0 and D_{r+1} (otherwise the support of γ' would contain a torus fixed point). We deduce that there exists an unique Cartier divisor γ_0 on $D + D_0 + D_{r+1}$ so that

$$\gamma_{0|D} = \gamma' \quad \text{and} \quad \gamma_{0|D_0+D_{r+1}} = C' \cdot D_0 + C' \cdot D_{r+1}$$

We have equality $D + D_0 + D_{r+1} = G - K_X$ and we obtain

$$\begin{aligned} H^1(X, \mathcal{O}_X(G_Q - D - D_0 - D_{r+1}) &\simeq H^1(X, \mathcal{O}_X(G_Q - G + K_X) \\ &\simeq H^1(X, \mathcal{O}_X(G - G_Q))\check{} \\ &\simeq H^1(X, \mathcal{O}_X(G_P))\check{} = 0. \end{aligned}$$

The second isomorphism is Serre Duality, and the last equality comes from the fact that the H^1 of a globally generated line bundle on a toric surface vanishes (see [14]). Last equality combined with the short exact sequence

$$0 \to \mathcal{O}_X(G_Q - D - D_0 - D_{r+1}) \to \mathcal{O}_X(G_Q) \to \mathcal{O}_{D+D_0+D_{r+1}}(\gamma_0) \to 0,$$

imply that there exists $C'' \in |\mathcal{O}_X(G_Q)|$ which restricts to γ_0 on $D + D_0 + D_{r+1}$. A fortiori, C'' restricts to γ' on D. Since $G_Q - D_Q = -\partial X < 0$, we have $H^0(X, \mathcal{O}_X(G_Q - D_Q)) = 0$. Thus $C' = C''$, the two curves having the same restriction to D_Q.

There remains to show that $C' \leq C$. Suppose that there exists an irreducible component C_0 of C' with proper intersection with C. Then, we can compute the intersection multiplicity of C_0 and C at any $p \in X$. It is given by

$$mult_p(C_0, C) = dim_{\mathbb{C}} \frac{\mathcal{O}_{X,p}}{(f_p, g_p)}$$

where f_p and g_p are respective local equations for C and C_0 at p. By assumption,

$$C_{0|D} \leq C_{|D}$$

so that the class of g_p in $\mathcal{O}_{D,p}$ divides that of f_p. We deduce that

$$f_p = u_p g_p + v_p h_p$$

for some holomorphic functions u_p, v_p, where h_p is a local equation for D. Thus, we obtain inequality

$$dim_{\mathbb{C}} \frac{\mathcal{O}_{X,p}}{(f_p, g_p)} \geq dim_{\mathbb{C}} \frac{\mathcal{O}_{X,p}}{(g_p, h_p)} = mult_p(C_0, D),$$

for all p in the support of D. Finally,

$$deg(\mathcal{O}_X(C_0))_{|C} \geq \sum_{p\in|D|} mult_p(C_0,C) \geq \sum_{p\in|D|} mult_p(C_0,D) = deg(\mathcal{O}_X(C_0))_{|D}.$$

Since D is rationally equivalent to $C+\partial X$, this implies that C_0 has a negative intersection with the boundary. This leads to a contradiction. Thus C_0 is necessarily an irreducible component of C. Finally $C' \leq C$, corresponding to a factor q of f with Newton polytope Q. Since $G_Q - D_Q < 0$, the restriction $H^0(\mathcal{O}_X(G_Q)) \to H^0(\mathcal{O}_{D_Q}(G_Q))$ is injective. Thus $C' \in |\mathcal{O}_X(G_Q)|$ can be uniquely recovered from its restriction $\gamma'_{|D_Q}$ to D_Q (and a fortiori from γ').

There remains to show that the given conditions do not depend on the choice of π. Let $\widetilde{X}, \widetilde{D}, \widetilde{\gamma}$ be the triplet associated to an other choice

$$\widetilde{X} \stackrel{\widetilde{\pi}}{\to} X_f$$

of desingularization. Since we can refine simultaneously both fans of X and $\widetilde{X}$, it's enough to show the independance of conditions when

$$\widetilde{X} \stackrel{b}{\to} X$$

is obtained from X by blowing up a torus fixed point of ∂X. The inverse-image of the boundary of X is thus equal to

$$b^{-1}(\partial X) = \partial\widetilde{X} + r\widetilde{E}$$

where $\widetilde{E}$ is the exceptional divisor of p and $r \geq 0$. The curve $\widetilde{C} \subset \widetilde{X}$ defined by f does not intersect E and $\widetilde{C} = b^{-1}(C)$ is isomorphic to C. We deduce that

$$b^{-1}(D) = \widetilde{D} + rE.$$

Since $\widetilde{C} \cap |E| = \emptyset$, the map b induces an isomorphism between the group of Cartier divisors $\widetilde{\gamma}'$ of $\widetilde{D}$ supported on $|\widetilde{D}\cdot\widetilde{C}|$, and the group of Cartier divisors γ' on D supported on $|D\cdot C|$, mapping $\widetilde{\gamma}$ to γ. In particular, $\gamma' \leq \gamma$ satisfies the degree hypothesis of Theorem 2 if and only if $\widetilde{\gamma}'$ does.

By Lemma 3, we have equality $P_{D+K_X} \cap \mathbb{Z}^2 = P_{\widetilde{D}+K_{\widetilde{X}}} \cap \mathbb{Z}^2$ so that the pull-back b^* on forms determines an isomorphism

$$H^0(X, \Omega^2_X(D)) \stackrel{b^*}{\to} H^0(\widetilde{X}, \Omega^2_{\widetilde{X}}(\widetilde{D}))$$

(see Subsection 2.5.3). Note that b^* commutes with the $\bar{\partial}$-operator.

Finally, keeping notations of the proof of Theorem 1, we obtain equality

$$\begin{aligned}
\langle\widetilde{\gamma}, \widetilde{\Psi}\rangle_p = \langle[\widetilde{\gamma}_p] \wedge \bar{\partial}[\widetilde{\psi})]\,,\, 1_{\widetilde{X}}\rangle &= \langle[\widetilde{\gamma}_p] \wedge \bar{\partial}[\widetilde{\psi})]\,,\, b^*(1_X)\rangle \\
&= \langle b_*\Big([\widetilde{\gamma}_p] \wedge \bar{\partial}[b^*(\psi)]\Big)\,,\, 1_X\rangle \\
&= \langle[\gamma_{b(p)}] \wedge \bar{\partial}[\psi]\,,\, 1_X\rangle = \langle\gamma, \Psi\rangle_{b(p)}
\end{aligned}$$

for all $\widetilde{\Psi} \in H^0(\widetilde{X}, \Omega^2_{\widetilde{X}}(\widetilde{D}))$ and all $p \in |\partial\widetilde{X}|$. This shows that conditions of Theorem 2 do not depend on the choice of the desingularization $\pi : X \to X_f$. □

Remark 1. *Since $0 \in \mathbb{C}^2 \subset X_f$ does not belong to $\pi(E)$, hypothesis (H_2) is not crucial. If we only assume that N_f intersects both coordinate axes, the osculating criterions still permit to detect an absolute factor q of f associated to the choice of*

a summand Q of N_f. Nevertheless, although the Newton polytope N_q of q still has the same exterior facets of Q, we now don't necessarily have equality $N_q = Q$.

3.3. **Computing the absolute factors of f.** Suppose that $\gamma' \leq \gamma$ satisfies conditions of Theorem 2 for a Minkowski summand Q of N_f. We give here an efficient way to compute the corresponding absolute factor q of f. The polynomial q admits the monomial $\mathbb{C}$-expansion

$$q(t) = \sum_{m \in Q \cap \mathbb{N}^2} a_m t^m,$$

and we look for the homogeneous class

$$[a] \in \mathbb{P}^{Card(Q \cap \mathbb{N}^2)-1}(\mathbb{C})$$

of the vector $a = (a_m)_{m \in Q \cap \mathbb{N}^2}$.

We denote by $\Gamma' = \gamma' \cdot \partial X$ and by $\Gamma'_i = \Gamma' \cdot D_i$. Let us fix $p \in |\Gamma'_i|$. If f satisfies hypothesis (H_1), we can define the complex numbers

$$\alpha_p(u,v) := \frac{\partial^u \phi_p^v}{\partial x_i^u}(0) \quad \text{if } u \geq 0, \qquad \alpha_p(u,v) := 0 \quad \text{if } u < 0,$$

for all integers u, v, where

$$y_i - \phi_p(x_i) = 0$$

is the Weirstrass equation of the germ of C at p (recall that $\phi_p(0) \neq 0$). For $k \in \mathbb{N}$ and $m \in \mathbb{Z}^2$, we then define the complex number

$$\beta_p(k,m) := \alpha_p(k - \langle m, \eta_i \rangle - e_i, \langle m, \eta_{i+1} \rangle + e_{i+1}),$$

where $e_i := -min_{m \in Q} \langle m, \eta_i \rangle$. We denote by $Vol(Q)$ the euclidean volume of Q in $\mathbb{R}^2$.

We obtain the following

Proposition 1. *Suppose that f satisfies (H_1) and (H_2). The homogeneous vector $[a]$ is uniquely determined by conditions*

$$\sum_{m \in Q \cap \mathbb{Z}^2} a_m \beta_p(k,m) = 0,$$

for all $p \in |\Gamma'_i|$, all $0 \leq k \leq e_i$ and all $i = 1, \ldots, r$.

The underlying linear system $(S_{\gamma'})$ contains $2Vol(Q) + deg(\Gamma')$ equations of $Card(Q \cap \mathbb{Z}^2)$ unknowns and can be constructed from the restriction of γ' to the divisor $G_Q + \partial X$.

Proof. It's well known that the curve $C' \in |\mathcal{O}_X(G_Q)|$ of q has affine polynomial equation

$$q_i(x_i, y_i) = \sum_{m \in Q \cap \mathbb{Z}^2} a_m x_i^{\langle m, \eta_i \rangle + e_i} y_i^{\langle m, \eta_{i+1} \rangle + e_{i+1}} = 0$$

in the chart $U_i = Spec\, \mathbb{C}[x_i, y_i]$ (see [11] for instance). By assumption,

$$q_i(x_i, \phi_p(x_i)) \equiv 0$$

for all $p \in |\Gamma'_i|$. It's easy to show that the k^{th}-derivative of this expression evaluated at 0 is equal to $c \times \sum_{m \in Q \cap \mathbb{Z}^2} a_m \beta_p(k,m)$ for a non zero scalar c. Thus the coefficients

of $[a]$ determine a non trivial solution of $(S_{\gamma'})$. Conversely, a non trivial solution $\widetilde{a}$ of $(S_{\gamma'})$ defines a polynomial

$$\widetilde{q}(t) = \sum_{m \in Q \cap \mathbb{N}^2} \widetilde{a}_m t^m$$

supported on Q, and which satisfies

$$\Big[\frac{\partial^k}{\partial x_i^k} \widetilde{q}_i(x_i, \phi_p(x_i))\Big]_{x_i=0} = 0$$

for all $p \in |\Gamma'_i|$, all $0 \leq k \leq e_i$ and all $i = 1, \ldots, r$. This is precisely equivalent to that the curve $\widetilde{C} \subset X$ of $\widetilde{q}$ osculates C' with order e_i at each $p \in |\Gamma'_i|$. We deduce that the restrictions of $\widetilde{C}$ and C' to $G_Q + \partial X = \sum_{i=1}^r (e_i + 1) D_i$ satisfy

$$C'_{|\sum e_i D_i + \partial X} \leq \widetilde{C}_{|\sum e_i D_i + \partial X}.$$

On an other side, the Newton polytope of $\widetilde{q}$ is included in Q. Thus, we necessarily have $deg(\widetilde{C} \cdot D_i) \leq deg(C' \cdot D_i)$ for all $i = 1, \ldots, r$. Combined with previous inequality, this forces equality $C' \cdot \partial X = \widetilde{C} \cdot \partial X$ and we deduce

$$C'_{|\sum e_i D_i + \partial X} = \widetilde{C}_{|\sum e_i D_i + \partial X}.$$

Since q has Newton polytope Q, the isomorphism (7) gives equality

$$\sum_{i=1}^r e_i D_i = div_\infty(q) =: G_Q.$$

The restriction map $H^0(X, \mathcal{O}_X(G_Q)) \to H^0(X, \mathcal{O}_{G_Q + \partial X}(G_Q))$ being injective, the two curves C' and $\widetilde{C}$ are equal and the polynomials q and $\widetilde{q}$ necessarily coincides up to multiplication by a non zero scalar. Thus $[a] = [\widetilde{a}]$.

We just saw that the linear system $(S_{\gamma'})$ only depends on the restriction of γ' to the divisor $G_Q + \partial X < D$. It contains precisely

$$\sum_{i=1}^r \sum_{p \in |\Gamma'_i|} (e_i + 1) = \sum_{i=1}^r (e_i + 1) deg(C' \cdot D_i) = deg(C' \cdot G_Q) + deg(C' \cdot \partial X)$$

equations. We have $deg(C' \cdot G_Q) = deg(C' \cdot C') = 2Vol(Q)$, where second equality follows from basic toric intersection theory [14]. □

Each linear equation involves a reduced number of unknowns and the linear system $(S_{\gamma'})$ has a very particular sparse structure. For instance, letting $k = 0$, we obtain for each $i = 1, \ldots, r$ the linear subsystem

$$\sum_{m \in Q^{(i)} \cap \mathbb{Z}^2} a_m [\phi_p(0)]^{\langle m, \eta_{i+1} \rangle + e_{i+1}} = 0, \ \forall \ p \in |\Gamma'_i|.$$

It has $Card(Q^{(i)} \cap \mathbb{Z}^2) - 1$ equations with $Card(Q^{(i)} \cap \mathbb{Z}^2)$ unknowns and permits to determine the coefficients of the i^{th} exterior facet poylomial of q. For $k = 1$, we deduce relations on the coefficients $\{a_m, \ \langle m, \eta_i \rangle + e_i = 1\}$. For a general k, we deduce relations on the coefficients $\{a_m, \ \langle m, \eta_i \rangle + e_i = k\}$.

3.4. **Sketch of a sparse vanishing-sums algorithm.** We describe here a possible sparse vanishing-sums algorithm associated to Theorem 2 and Proposition 1. When we say compute, we mean compute by using floatting calculous with a given precision. When we say test a vanishing-sum, we mean test an $\leq \epsilon$-sum for an arbitrary small $\epsilon > 0$. The smaller ϵ is, the bigger number of necessary digits is.

Input: A polynomial $f \in K[t_1, t_2]$ which satisfies $f(0,0) \neq 0$ and with square free exterior facet polynomials.

Output : The irreducible factorization of f over $\mathbb{C}$.

Step 1. Compute the Minkowski summands of N_f. Use for instance the algorithm presented in [16]. If N_f is irreducible, so is f. Otherwise go to step 2.

Step 2. Compute the fan of X. The fan Σ is obtained from Σ_f by adding some rays in the singular two-dimensional cones of Σ_f. Such a fan can be obtained in a canonical way by using an Euclidean algorithm, or by computing some Hirzebruch-Jung continued fraction (see [14]).

Step 3. Compute the osculating data (D, γ). By Lemma 3, we have equality

$$D = \sum_{i=1}^{r} (k_i + 1) D_i, \quad k_i := -min_{m \in N_f} \langle m, \eta_i \rangle.$$

The Cartier divisor γ on D is obtained by computing the family of implicit functions $\{\phi_p,\ p \in |\Gamma_i|\}$ up to order k_i, for $i = 1, \ldots, r$. Recall that $\Gamma_i = 0$ when ρ_i is not an exterior ray of N_f.

Step 4. Compute the Newton polytopes of the absolute irreducible factors. The osculating conditions (2) are given by the explicit vanishing-sums (8). Then, Theorem 2 gives an efficient way to compute the decompositions

$$\gamma = \gamma_1 + \cdots + \gamma_s, \qquad N_f = Q_1 + \cdots + Q_s$$

of γ and N_f associated to the irreducible absolute decomposition $f = q_1 \cdots q_s$ of f.

Step 5. Compute the irreducible absolute factors of f. Use Proposition 1. The coefficients of the linear systems (S_{γ_i}), $i = 1, \ldots, s$ are linear combination of the residues $\langle \gamma, \Psi_m \rangle_p$, $m \in Q \cap (\mathbb{N}^*)^2$ already computed in step 4.

The numerical part of the algorithm reduces to the computation of the roots of the univariate exterior facet polynomials of f. Then it detects the absolute factorization of f with a probability which increases after each positive vanishing-tests, up to obtain the adequat decomposition of N_f. Then the associated factors are easily computed. Roughly speaking, this method corresponds to a toric version of the Hensel lifting. A comparable algorithm has been obtained by Abu Salem-Gao-Lauderin in [1], by using combinatorial tools.

If we can decide formally if a sum vanishes, there is no chance of failure in step 4 and the algorithm is deterministic. If we test the osculating criterions (8) for a generic linear combination of the involved m's, the Newton polytope decomposition is valid only with probability one, in the vain of the Galligo-Rupprecht and Elkadi-Galligo-Weimann algorithms [13] or [12].

Nevertheless, as in [13] and [12], our algorithm necessarily uses $\leq \epsilon$-sum tests imposed by floatting calculous and numerical approximation. Thus, it can happen that the Newton decomposition of N_f in step 4 does not correspond to the absolute

decomposition of f (and that for any choice of $\epsilon > 0$) and there is a chance of failure of the algorithm. Nevertheless, in the important case a polynomial f defined and irreducible over $\mathbb{Q}$ the authors in [7] show that we can recover the exact factorization with formal coefficients in a finite extension of K from a sufficiently fine approximate factorization. This problem will be explored in a further work.

3.5. **Comparison with related results.** Let us compare our algorithm with related factorization algorithms.

3.5.1. *Comparison with the Galligo-Rupprecht GR-algorithm.* In [13], the authors perform a generic change of affine coordinates and then compute the factorization of f

$$f(t_1, t_2) = \prod_{i=1}^{d} (t_2 - \phi_i(t_1))$$

in $\mathbb{C}\{t_1\}[t_2]$ up to precision t_1^3. They detect the factors of f with probability one by testing the Reiss relation (3) on subfamilies $\mathcal{F} \subset \{\phi_i,\, i = 1, \ldots, d\}$. Then they use the Hensel lemma in order to lift and compute the candidate factors. Let us compare this algorithm with our approach.

About the recombination number. We define the recombination number $\mathcal{N}(f)$ to be the maximal number of choices $\gamma' < \gamma$ necessary to detect the absolute factorization of f in step 4. By (10), it depends on the geometry of N_f and is subject to constraints given by the possible Minkowski-sum decompositions of N_f. For instance, if f is irreducible over K, its irreducible absolute factors necessarily have *the same polytope* (see [8] for instance) and $\mathcal{N}(f)$ decreases drastically.

We denote by $\mathcal{M}(f)$ the recombination number of the GR-algorithm, that is the number of possible choices for the families $\mathcal{F}$ when taking in account restrictions imposed by the possible Minkowski-sums decompositions of N_f. We prove here the following improvement

Lemma 4. *Suppose that f is irreducible over K and satisfies hypothesis (H_1) and (H_2). Let $d = deg(f)$. Then*

$$\mathcal{N}(f) \leq \mathcal{M}(f) \leq 2^{deg(f)}$$

with equivalence

$$\mathcal{N}(f) = \mathcal{M}(f) \iff N_f = Conv\{(0,0), (d,0), (0,d)\}.$$

Proof. let n be the biggest integer so that $N_f = nQ_0$ for a lattice polytope Q_0. Thus $deg(f) = nl$ where l is the total degree of a polynomial with polytope Q_0. By [8], an irreducible absolute factor of f has Newton polytope kQ_0 for some integer k which divides n and the GR-algorithm looks for an irreducible factor of degree kl. This gives the recombination number

$$\mathcal{M}(f) = \sum_{k|n} C_{kl}^{nl},$$

where C_j^i is the usual number of combinations. We clearly have $\mathcal{M}(f) \leq 2^{deg(f)}$. Equality $\mathcal{M}(f) = 2^{deg(f)}$ holds if and only if f is a dense polynomial which is not assumed to be irreducible over K.

Denote now by $l_1, \dots, l_t$ the lattice lenght of the exterior facets of Q_0. Then, restrictions (10) imposed to the possible choice of $\gamma' \leq \gamma$ induce equality

$$\mathcal{N}(f) = \sum_{k|n} \prod_{i=1}^{t} C_{kl_i}^{nl_i}.$$

We have both inequalities

$$\prod_{i=1}^{t} C_{kl_i}^{nl_i} \leq C_{k(l_1+\cdots+l_t)}^{n(l_1+\cdots+l_t)} \quad \text{and} \quad C_{k(l_1+\cdots+l_t)}^{n(l_1+\cdots+l_t)} \leq C_{kl}^{nl}$$

for any $k \leq n$. First inequality is an equality if and only if there is only $t = 1$ exterior facet, and the difference strictly increases with t. Second inequality follows from the fact that the sum

$$l_f = nl_1 + \cdots + nl_t$$

of the lattice lenght of the exterior facets of N_f is smaller or equal to $deg(f)$. Moreover, we can convince that there is equality $l_f = deg(f)$ if and only if the normal fan Σ_f of N_f is regular. This is of course exceptional, and $l_f << deg(f)$ in general. Finally, we have $\mathcal{N}(f) \leq \mathcal{M}(f)$ and equality holds if and only if N_f is regular with one exterior facet. Since $0 \in N_f$ by assumption, this is equivalent to that $N_f = Conv\{(0,0),(d,0),(0,d)\}$. □

Note that there are fast factorization algorithms over a number field K (see [4], [26]). The following example illustrates Lemma 4.

Example 3. Suppose that f is irreducible over K and that $N_f = nQ_0$, where Q_0 is the "undivisible" lattice polytope

$$Q_0 = Conv\{(0,0),(a-1,0),(0,a-1),(a,a)\},$$

with $a \geq 2$ and n prime. The lattice lenghts of the $t = 2$ exterior facets of N_f are both equal to n. Since n is prime, the underlying recombination number is equal to

$$\mathcal{N}(f) = n^2.$$

In particular, is does not depend on a. The GR-algorithm considers f as a dense polynomial of degree $deg(f) = 2na$ and looks for an irreducible absolute factor of degree $2a$. The induced recombination number $\mathcal{M}(f)$ is thus equal to

$$\mathcal{M}(f) = C_{2a}^{2an} \simeq \frac{2a^{2a}}{(2a)!} n^{2a},$$

and growths exponentially with a.

The asymptotic estimation of $\mathcal{N}(f)$ for a "generic polytope"[1] N_f is a difficult problem. It is related to the estimation of the number of exterior facets, and to the estimation of "how singular" is the normal fan. Geometrically, these numbers correspond to the Picard numbers of X_f and of a minimal resolution X.

Note that by Lemma 3 and Theorem 2, the maximal number of vanishing-sums to test is equal to

$$Card(N_f \cap (\mathbb{N}^*)^2) \times \mathcal{N}(f).$$

[1]The genericity has to be defined relatively to some invariant, as the cardinality of interior lattice points, or the volume for instance.

If we only want to detect absolute factors with probability 1, it's enough to test (8) on a generic linear combination of the involved $m \in N_f \cap \mathbb{Z}^2$. In such a case, it's enough to test $\mathcal{N}(f)$ vanishing-sums.

About the numerical part. The numerical part of our algorithm reduces to the computation of the roots of the exterior facet univariate polynomials. It's faster to factorize t univariate polynomials of degree $l_1, \ldots, l_t$ than an univariate polynomial of total degree $l_f \geq l_1 + \cdots + l_t$. Thus, the computation of $C \cdot \partial X$ is faster than with a generic line as soon as $\mathcal{N}(f) < \mathcal{M}(f)$.

About the lifting step. Although we need to compute a reduced number implicit functions, we need *in general* a bigger precision on the ϕ_p's than the upper bound $deg(f)$ precision required with the classical Hensel lifting. In Example 3, we need for instance to compute the ϕ_p's up to order $na^2 >> 2na = deg(f)$. Morally, the more the recombination number is reduced, the more the required precision on the ϕ_p's increases. Thus, we should be very carefull when comparing algorithmic complexity. Nevertheless, we gain on both sides in the important case of a polynomial of bidegree (a, b). Formula (8) shows that we need to compute a and b implicit functions up to respective maximal orders b and a, while the GR-algorithm computes $a+b$ implicit functions up to a maximal order $a + b$.

3.5.2. *Comparison with the Elkadi-Galligo-Weimann EGW-algorithm.* In [12], the authors develop the sketch of an algorithm with the same recombination number that here by using the interpolation criterions obtained in [31]. Their approach necessites to compute numerically the intersection of $C \subset X$ with a *generic* curve L in a very ample linear system which is "close enough" to $|\partial X|$. In other words, they pick a Newton polytope P whose normal fan is that of X and then solve a polynomial system $f = \epsilon p + 1 = 0$, where p has polytope $N_p = P$ and ϵ is a small positive real number. When ϵ goes to 0, the roots of the system go to the boundary of X and they deduce an asymptotic distribution of the zero-cycle $C \cdot L$ which traduces the polytopal information. Roughly speaking, Theorem 2 corresponds to the limit case $\epsilon = 0$. A great advantage is that we avoid the delicate problem of the "small enough ϵ" choice and of the asymptotic distribution lecture. As in the GR-algorithm, the generic choice of p permits to compute $deg(C \cdot L)$ implicit functions only up to order 2 in order to detect the absolute decomposition of f with probability one. Here, we compute only $deg(C \cdot \partial X) << deg(C \cdot L)$ implicit functions, but with a bigger precision. We detect the absolute decomposition of f deterministically.

3.6. **Using non toric information.** Suppose that C is reduced, but with singularities along the boundary of X (so the exterior facet polynomials of f have square absolute factors). Thus $\Gamma = C \cdot \partial X$ is non reduced and the computations of residues is much more delicate. In particular, we can not use formula (8).

Nevertheless, there exists in such a case a (non toric) smooth completion $\widetilde{X}$ of $\mathbb{C}^2$ obtained from X by a serie of blow-ups, and so that the proper transform $\widetilde{C} \subset \widetilde{X}$ of C has a transversal intersection with the boundary of $\widetilde{X}$. By choosing an effective divisor $\widetilde{D}$ supported on $\partial\widetilde{X}$ and with sufficiently big multiplicities, we can then use Theorem 1 efficiently to decompose $\widetilde{C}$ and to recover the absolute factorization of f. The added exceptional divisors give new restrictions on the possible choices of

$\widetilde{\gamma}' < \widetilde{\gamma}$ (where $\widetilde{\gamma} = \widetilde{C}_{|\widetilde{D}}$) and the presence of singularities of C along ∂X finally turns out to be an opportunity to reduce the recombination number. There remains to find the best choice for $\widetilde{D}$.

3.7. **Conclusion.** We propose a new algorithm which computes the absolute factorization of a bivariate polynomial by taking in account the geometry of the Newton polytope. For a sparse polynomial, this permits to reduce the recombination number when compared to the usual vanishing-sums algorithms. There remains to implement such an algorithm and to compute formally its complexity. This is the object of a further work. What we'll remind here is the general idea that

The more a curve is singular, the more it is easy to decompose.

For a sparse polynomial f, a naive embedding of the curve of f in $\mathbb{P}^2$ produces many toric singularities on the line at infinity, and we have shown here that an adequat toric resolution X permits to use this sparse information. Moreover Theorem 1 permits in theory to profit also of *non toric* singularities of C on the boundary of X. This too will be explored in a further work.

References

[1] F. Abu Salem, S. Gao, A.G.B. Lauder, *Factoring polynomials via polytopes*, proc. of ISSAC (2004), pp. 411.

[2] M. Andersson, *Residue currents and ideal of holomorphic functions*, Bull. Sci. math. (2004), pp. 481-512.

[3] M. Avendano, T. Krick, M. Sombra, *Factoring bivariate sparse (lacunary) polynomials*, J. Complexity 23 (2007), pp. 193-216.

[4] K. Belabas, M. van Hoeij, J. Kluners, A. Steel, *Factoring polynomials over global fields*, Manuscrit (2004).

[5] W.P. Barth, K. Hulek, C.A.M. Peters, A. Van De Ven, *Compact Complex Surfaces*, Springer-Verlag, Second Edition (2004).

[6] A. Bostan, G. Lecerf, B. Salvy, E. Schost, B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, proc. of ISSAC (2004), pp. 42-49.

[7] G. Chèze, A. Galligo, *From an approximate to an exact factorization*, J. Symbolic Computation, 41, no. 6 (2006), pp. 682-696.

[8] G. Chèze, *Absolute polynomial factorization in two variables and the knapsack proble*, proc. of ISSAC (2004), pp. 87-94.

[9] G. Chèze and G. Lecerf, *Lifting and recombination techniques for absolute factorization*, J. of Complexity 23, no. 3 (2007), pp. 380-420.

[10] D. Cox, *The homogeneous coordinate ring of a toric variety*, J. Algebraic Geom. 4 , no. 1 (1995), pp. 17-50.

[11] V. Danilov, *The geometry of toric varieties*, Russian Math. Surveys 33 (1978), pp. 97-154.

[12] M. Elkadi, A. Galligo, M. Weimann, *Towards Toric Absolute Factorization*, J. Symb. Comp. (2009), doi:10.1016/j.jsc.2008.03.007.

[13] A. Galligo, D. Rupprecht, *Irreducible decomposition of curves*, J. Symb. Comp., 33 (2002), pp. 661-677.

[14] W. Fulton, *Introduction to Toric Varieties*, Annals of Math. Studies, Princeton University Press (1993).

[15] S. Gao, *Factoring multivariate polynomials via partial differential equation*, Math. Comp. 72, no 242 (2003), pp. 801-822.

[16] S. Gao, A.G.B. Lauder, *Decomposition of polytopes and polynomials*, Disc. and Comp. Geom. 6, no1 (2001), pp. 89-104.

[17] J. von zur Gathen, J. Gerhard, *Modern computer algebra*, Cambridge University Press, 1st edition (1999).

[18] M.L. Green, *Secant functions, the Reiss relation and its converse*, Trans. of Amer. Math. Soc. 280, no.2 (1983), pp. 499-507.

[19] P.A. Griffiths, *Variations on a theorem of Abel*, Inventiones Math. 35 (1976), pp. 321-390.

[20] P.A. Griffiths, J. Harris, *Principles of Algebraic Geometry*, Pure and applied mathematics, Wiley-Intersciences (1978).
[21] P.A. Griffiths, J. Harris, *Residues and zero-cycles on algebraic varieties*, Annals of Math. 108 (1978), pp. 461-505.
[22] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag (1977).
[23] G. Henkin, M. Passare, Abelian differentials on singular varieties and variation on a theorem of Lie-Griffiths, Inventiones math. 135, 297-328, 1999.
[24] A.G. Khovansky, *Newton polyhedra and toric varieties*, Funct. Anal. Appl. 11 (1977), pp. 56-67.
[25] G. Lecerf, *Sharp precision in Hensel lifting for bivariate polynomial factorization*, Math. Comp. 75 (2006), pp. 921-933.
[26] G. Lecerf, *Improved dense multivariate polynomial factorization algorithms*, J. Symb. Comp. (2007), to appear.
[27] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovsz, *Factoring Polynomials with Rational Coefficients*, Math. Ann. 261, no.2 (1982), pp. 515-534.
[28] A.M. Ostrowski, *On multiplication and factorization of polynomials. Lexicographic orderings and extreme aggregates of terms*, Aequationes Math. 13 (1975), pp. 201-228.
[29] D. Rupprecht, *Semi-numerical absolute factorization of polynomials with integer coefficients*, J. Symbolic Computation 37 (2004), pp.557-574.
[30] A. Tsikh, *Multidimensional residues and their applications*, Transl. Amer. Math. Soc 103, (1992).
[31] M. Weimann, *Trace et calcul résiduel: nouvelle version du théorème d'Abel-inverse et formes abéliennes*, Ann. de Toulouse, 16, no.2 (2007), pp. 397-424.
[32] M. Weimann, *An interpolation theorem in toric varieties*, Ann. Inst. Fourier 58, no.4 (2008), pp. 1371-1381.
[33] J.A. Wood, *A simple criterion for an analytic hypersurface to be algebraic*, Duke Math. J. 51 (1984), pp. 235-237.
[34] J.A. Wood, *Osculation by Algebraic Hypersurfaces*, J. Differential Geometry 18 (1983), pp. 563-573.

Departament Algebra i Geometria, Facultat de Matemàtiques, Universitat Barcelona Gran via 585, 08007 Barcelona.
E-mail address: weimann23@gmail.com