



# Algebraic Osculation and Application to Factorization of Sparse Polynomials

Martin Weimann

## ► To cite this version:

Martin Weimann. Algebraic Osculation and Application to Factorization of Sparse Polynomials. Foundations of Computational Mathematics, 2012, 12 (2), pp.173-201. 10.1007/s10208-012-9114-z . hal-02137318

**HAL Id: hal-02137318**

**<https://normandie-univ.hal.science/hal-02137318>**

Submitted on 22 May 2019

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

---

# ALGEBRAIC OSCULATION AND APPLICATION TO FACTORIZATION OF SPARSE POLYNOMIALS

by

Martin Weimann

---

**Abstract.** — We prove a theorem on algebraic osculation and 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 the boundary  $\partial X = X \setminus \mathbb{C}^2$ . Our main result gives explicit conditions that are necessary and sufficient for a given Cartier divisor on the subscheme  $(|D|, \mathcal{O}_D)$  to extend to  $X$ . These osculation criterions are expressed with residues. When applied to the toric setting, our result gives rise to a new algorithm for factoring sparse bivariate polynomials which takes into account the geometry of the Newton polytope.

## 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 criteria for algebraic osculation in toric varieties.

Since the 1980s, 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 - referred to here as LR-algorithms - are based on a *Lifting and Recombination* scheme, which detects the 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* necessitates an exponential number of possible recombinations, researchers succeeded in the last decade to develop LR-algorithms running now in a quasi-optimal polynomial complexity (see for instance [8], [9] and the reference therein).

In general, an LR-algorithm needs 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 carried by the Newton polytope  $N_f$  of  $f$ .

---

**2000 Mathematics Subject Classification.** — classification .

**Key words and phrases.** — Mots-clefs dans la langue de l'article .

We propose here a new method which avoids this generic change of coordinates. We use an osculation criteria at the toric infinity in order to detect and compute the irreducible absolute factors of  $f$  from the factorization of its univariate facet polynomials lifted to analytic factors with a suitable precision. This allows us to use the geometry of the Newton polytope and to reduce the number of possible recombinations of the local factors when compared to the Galligo-Rupprecht algorithm [13]. This approach recently led to the first deterministic algorithm that factors rational bivariate polynomials in small polynomial time in the volume of the Newton polytope (see [33]). Let us present our main results.

**Algebraic Osculation.** A natural way to take advantage of 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  $f$  and we want to use this information. The boundary  $\partial X = X \setminus \mathbb{C}^2$  of  $X$  is a normal crossing divisor whose Picard group satisfies

$$\mathrm{Pic}(\partial X) \simeq \mathrm{Pic}(X).$$

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 when a Cartier divisor on  $D$  extends to  $X$ . This is achieved in our main result:

**Theorem 1.1.** — *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  $\Omega_X^2(D)$  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  $H^0(X, \Omega_X^2(D))$  with the property that a Cartier divisor  $\gamma$  on  $D$  extends to a Cartier divisor  $E$  on  $X$  if and only if*

$$(1) \quad \langle \gamma, \Psi \rangle = 0 \quad \forall \Psi \in H^0(X, \Omega_X^2(D)).$$

*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 subscheme extensions). When  $X$  is a toric surface we obtain an explicit formula for  $\langle \gamma, \Psi \rangle$ , generalizing a theorem of Wood [35] who considers the projective case  $X = \mathbb{P}^n$ . Although the proof of Wood's theorem follows from a direct calculation in a unique affine chart, the proof of Theorem 1.1 requires to compute the cohomological obstruction to extend line bundles from  $D$  to  $X$ . We use then the Dolbeault  $\bar{\partial}$ -resolution and the residue currents to make explicit the conditions.

**Application to polynomial factorization.** If two algebraic curves of fixed degree osculate each other with sufficiently large contact orders on some finite subset, they

necessarily have a common component. This basic observation permits us to derive from Theorem 1.1 an algorithm which computes the absolute factorization of a bivariate polynomial  $f$ . The polynomial  $f$  is assumed to be defined over a subfield  $K \subset \mathbb{C}$  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 prove the following result (Subsection 3.2):

**Theorem 1.2.** — *There exists a unique effective divisor  $D$  with support  $|\partial X|$  and rationally equivalent to  $C + \partial X$ . Let  $\gamma$  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*

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

*and so that the osculation conditions (1) hold for the pair  $(D, \gamma')$ . The factor  $q$  is computed from  $\gamma'$  by solving a sparse linear system of  $2 \text{Vol}(Q) + \deg(\gamma' \cdot \partial X)$  equations and  $\text{Card}(Q \cap \mathbb{Z}^2)$  unknowns.*

When the facet polynomials (Subsection 3.1) of  $f$  are square-free over  $\bar{K}$ , we can derive from Theorem 1.2 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 floating point computations 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 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]) and the number of possible recombinations decreases when compared to the Galigo-Rupprecht algorithm [13]. Let us mention that Theorem 1.1 concerns also non-toric

$\mathbb{C}^2$ -completions. This permits in theory to take advantage of the singularities of  $C$  along the boundary of  $X$  when  $f$  has non-reduced facet polynomials (see Subsection 3.6).

**Related results.** Our results constitute the heart of a deterministic algorithm developed later by the author in [33] for factoring rational bivariate polynomials in low-degree polynomial time in the volume of the Newton polytope. Our method is inspired by an originally work of the author with M.Elkadi and A.Galligo [12] where we use toric interpolation criterions [32] in an open neighborhood of  $\partial X$  (see Subsection 3.5). By using tools from combinatorics, the authors in [1] obtain a comparable facet lifting process which takes too into account the geometry of the Newton polytope, but no efficient complexity bounds are given. In [3], the authors reduce the factorization of a sparse polynomial to smaller dense factorizations in polynomial time in the input size.

**Organization.** The article is organized as follows. 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 give the precise statement of Theorem 1.1 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 1.2 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 algorithmic 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.

**Acknowledgment.** We would like to thank Michel Brion, Stéphane Druel, José Ignacio Burgos and Martin Sombra for their helpful comments. We also thank Mohamed Elkadi and André Galligo who suggested to us to pay attention to the interplay between toric geometry and sparse polynomial factorization.

## 2. Algebraic osculation

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

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

is the disjoint union of an affine plane  $X_0 \simeq \mathbb{C}^2$  with 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  $\partial X$ .

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

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

is an effective divisor with support  $|D| = |\partial X|$  and  $\gamma$  is a Cartier divisor on the subscheme  $(|D|, \mathcal{O}_D)$ . For convenience, we will identify  $D$  and the subscheme  $(|D|, \mathcal{O}_D)$ .

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

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

where  $i : D \rightarrow X$  is the inclusion map. In other words, we are looking for a divisor  $E$  with prescribed 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  $\gamma$  has support  $|\Gamma|$ , where  $\Gamma$  designs the zero-cycle  $\gamma \cdot \partial X$ . Thus,  $\gamma$  can be uniquely written as a finite sum

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

each  $\gamma_p$  being the restriction to  $D$  of a germ of an analytic *cycle* of  $X$  at  $p$

$$\tilde{\gamma}_p = \text{div}(f_p),$$

with  $f_p$  a germ of meromorphic function. When  $\tilde{\gamma}_p$  is smooth and intersects transversally  $\partial X$ , a curve restricts to  $\gamma_p$  at  $p$  if and only if it has contact order at least  $k_p$  with  $\tilde{\gamma}_p$ , 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  $\Omega_X^2$  be the canonical bundle of  $X$ . We identify the line bundle  $\Omega_X^2(D)$  with the sheaf of meromorphic forms with polar locus bounded by  $D$ . Thus, any global section  $\Psi$  of  $\Omega_X^2(D)$  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  $\psi$  on  $X$  such that

$$\Psi|_{X_0} = d\psi|_{X_0}.$$

For  $p \in |\Gamma|$ , we denote by  $\psi_p$  the germ of  $\psi$  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 2-form  $df_p \wedge \psi_p / f_p$  as

$$(2) \quad \text{res}_p \left[ \frac{df_p}{f_p} \wedge \psi_p \right] := \lim_{\epsilon \rightarrow 0} \frac{1}{(2i\pi)^2} \int_{u_p(\epsilon)} \frac{df_p}{f_p} \wedge \psi_p,$$

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 the Stokes theorem, it only depends on  $d\psi = \Psi$ . Moreover, the transformation law [20] implies that (2) only depends on  $f_p$  modulo  $(h_p)$ . That is, (2) depends on  $\gamma_p$  and not

on the chosen lifting  $\tilde{\gamma}_p = \{f_p = 0\}$ . By linearity, we can extend (2) to any germ of analytic cycle  $\tilde{\gamma}_p = \text{div}(f_p)$  and it follows finally that (2) defines a bilinear operator

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

between the group of Cartier divisor of  $D$  and the  $\mathbb{C}$ -vector space  $H^0(X, \Omega_X^2(D))$ . We refer to the proof of Theorem 1.1 (Subsection 2.4) for more details.

**2.3. Criteria for algebraic osculation.** — We keep previous notations. Our main result is the following precise formulation of Theorem 1.1:

**Theorem 2.1.** — *Let  $X$  be a smooth projective completion of  $\mathbb{C}^2$  with a normal crossing boundary  $\partial X$  and consider an osculating data  $(D, \gamma)$  on  $\partial X$ .*

1. *There exists a Cartier divisor  $E$  on  $X$  which restricts to  $\gamma$  on  $D$  if and only if*

$$(3) \quad \sum_{p \in |\Gamma|} \langle \gamma, \Psi \rangle_p = 0 \text{ for all } \Psi \in H^0(X, \Omega_X^2(D)).$$

*The divisor  $E$  is unique up to rational equivalence.*

2. *If moreover  $\gamma$  is effective and*

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

*then there exists an effective divisor of  $X$  which restricts to  $\gamma$  on  $D$ .*

The necessity of (3) follows from the theorem of residues [20]. The difficult part consists in showing that these conditions are also sufficient. The proof will be given in the next Subsection 2.4. Let us first illustrate Theorem 2.1 on a simple example.

**Example 2.2.** — (The Reiss relation). Let  $X = \mathbb{P}^2$  and consider a finite collection of  $d > 0$  smooth analytic germs  $\tilde{\gamma}_p$  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  $\geq 2$ . This problem leads to the osculation data  $(D, \gamma)$ , where  $D = 3L$  and  $\gamma$  is the restriction to  $D$  of  $\sum_{p \in |\Gamma|} \tilde{\gamma}_p$ . There is an isomorphism

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

and we can check that a generator is given by the form  $\Psi$  whose restriction to  $\mathbb{C}^2 = \mathbb{P}^2 \setminus L$  is equal to  $\Psi|_{\mathbb{C}^2} = dt_1 \wedge dt_2$  in affine coordinates  $(t_1, t_2)$ . Thus we can choose  $\psi|_{\mathbb{C}^2} = t_1 dt_2$ . Letting  $t_1 = T_1/T_0$  and  $t_2 = T_2/T_0$  we obtain

$$\psi = \frac{T_1(T_0 dT_2 - T_2 dT_0)}{T_0^3}$$

in the  $\mathbb{P}^2$  homogeneous coordinates  $[T_0 : T_1 : T_2]$ . Up to an affine change of coordinates, we can suppose that  $\gamma$  is supported in the affine chart  $T_2 \neq 0$ . In the new affine coordinates  $x = T_0/T_2$  and  $y = T_1/T_2$ , the line  $L$  has local equation  $x = 0$  and  $\psi = -y dx/x^3$ . Moreover, we can choose a Weierstrass equation

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

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

$$\operatorname{res}_p \left[ \frac{y dx \wedge d(y - \phi_p)}{x^3(y - \phi_p)} \right] = \operatorname{res}_0 \left[ \phi_p(x) \frac{dx}{x^3} \right] = \frac{1}{2} \phi_p''(0),$$

where  $\operatorname{res}_0$  is a univariate residue and  $\phi_p''$  is the second derivative of  $\phi_p$ . Finally, (3) is here equivalent to that

$$(4) \quad \sum_{p \in |\Gamma|} \phi_p''(0) = 0.$$

For degree reasons, any osculating divisor is rationally equivalent to  $dL$ . Since  $H^1(\mathcal{O}_{\mathbb{P}^2}(d-3)) = 0$ , the relation (4) is finally equivalent to that there exists an osculating curve  $C$  for  $(D, \gamma)$ .

It's easy to see directly the necessity of (4). 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  $\tilde{\gamma}_p$  with contact order 2, then  $\phi_p$  and  $u_p$  have the same Taylor expansion up to order 2, which directly shows necessity of (4). 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 2.1.** — Let us give first a brief overview of the proof. The given Cartier divisor  $\gamma$  on  $D$  corresponds to a line bundle  $\mathcal{L} \in \operatorname{Pic}(D)$  together with a global meromorphic section  $f$  of  $\mathcal{L}$ . An osculating divisor  $E$  for the pair  $(D, \gamma)$  corresponds to a line bundle  $\tilde{\mathcal{L}} \in \operatorname{Pic}(X)$  together with a global meromorphic section  $\tilde{f}$  which restrict respectively to  $\mathcal{L}$  and  $f$  on  $D$ . The problem of lifting the section  $f$  will follow easily from the Serre vanishing theorem. Thus, in order to extend  $\gamma$  from  $D$  to  $X$ , the main point is to understand the cokernel of the restriction map  $\operatorname{Pic}(X) \rightarrow \operatorname{Pic}(D)$ . By using the exponential sequences of  $D$  and  $X$  and Čech cohomology, we show first that we can associate to the line bundle  $\mathcal{L}$  a cocycle  $\zeta \in H^2(X, \mathcal{O}_X(-D))$  such that  $\mathcal{L}$  extends from  $D$  to  $X$  if and only if  $\zeta = 0$ . Then, we use the Dolbeault  $\bar{\partial}$ -resolution of the sheaf  $\Omega_X^2$  and residue currents in order to make explicit the Serre Duality Pairing between the two vector spaces  $H^2(X, \mathcal{O}_X(-D))$  and  $H^0(X, \Omega_X^2(D))$ . One obtains in such a way the formula (3) of Theorem 2.1. The second point of Theorem 2.1 follows directly from basic exact sequences.

Let us come now to the proof of Theorem 2.1. 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. The following lemma gives the cohomological obstruction for extending the line bundle  $\mathcal{L}$  from  $D$  to  $X$ .



**Lemma 2.3.** — *There is a decomposition of  $\text{Pic}(D)$  in a direct sum*

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

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

$$(5) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}_X & \longrightarrow & \mathcal{O}_X & \xrightarrow{\exp(2i\pi \cdot)} & \mathcal{O}_X^* \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathbb{Z}_D & \longrightarrow & \mathcal{O}_D & \longrightarrow & \mathcal{O}_D^* \longrightarrow 0 \end{array}$$

where  $\mathbb{Z}_D \subset \mathcal{O}_D$  is the subsheaf of  $\mathbb{Z}$ -valued functions (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

$$(6) \quad \begin{array}{ccccccc} & & 0 & \longrightarrow & \text{Pic}(X) & \xrightarrow{\delta_X} & H^2(X, \mathbb{Z}_X) \longrightarrow 0 \\ & & \downarrow & & \downarrow r & & \downarrow r' \\ H^1(D, \mathbb{Z}_D) & \longrightarrow & H^1(D, \mathcal{O}_D) & \xrightarrow{e} & \text{Pic}(D) & \xrightarrow{\delta_D} & H^2(D, \mathbb{Z}_D) \longrightarrow H^2(D, \mathcal{O}_D). \end{array}$$

Here  $r, r'$  are restriction maps,  $\delta_D, \delta_X$  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. Let  $j : X_0 \rightarrow X$  be the inclusion map of  $X_0 = X \setminus |D|$ . The short exact sequence

$$(7) \quad 0 \rightarrow j_!(\mathbb{Z}_{X_0}) \rightarrow \mathbb{Z}_X \rightarrow \mathbb{Z}_{|D|} \rightarrow 0$$

gives rise to the long exact cohomological sequence

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

where  $H_c^*(X_0)$  is the compact support cohomology of  $X_0$ . The cohomology  $H_c^*(X_0)$  is dual to the singular homology  $H_*(X_0)$  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  $\text{Pic}(X)$  is a direct summand of  $\text{Pic}(D)$ . The exponential cohomological sequence for  $X$  is exact in degree 0 so that  $H^1(X, \mathbb{Z}_X) \rightarrow H^1(X, \mathcal{O}_X)$  is injective and  $H^1(X, \mathbb{Z}_X) = 0$ . We have just seen that  $H_c^2(X_0) = 0$ , and finally (7) implies  $H^1(|D|, \mathbb{Z}_{|D|}) = 0$ . It follows that  $\ker(\delta_D) \simeq H^1(D, \mathcal{O}_D)$ .  $\square$

In all what follows, one keeps the notations of the proof of Lemma 2.3.

**Corollary 2.4.** — *There is an isomorphism  $\text{Pic}(X) \simeq \text{Pic}(\partial X)$ .*

*Proof.* — By Lemma 2.3, 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  $D$ . Since  $H^1(Z, \mathbb{Z}_Z) = 0$  for a finite set  $Z$ , there is a surjection

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

Since  $H^1(|D|, \mathbb{Z}_{|D|}) = 0$  by the proof of Lemma 2.3, one thus has  $H^1(D_i, \mathbb{Z}_{D_i}) = 0$  for all  $i$  and each  $D_i$  is a *rational* curve. In particular,  $H^1(\mathcal{O}_{D_i}) = 0$ . Moreover,  $H_c^1(X_0) = 0$  so that  $H^0(X, \mathbb{Z}_X) \rightarrow H^0(|D|, \mathbb{Z}_{|D|})$  is surjective and  $|D|$  is connected. Since  $D$  is simply connected too (because  $H^1(|D|, \mathbb{Z}_{|D|}) = 0$ ), one obtains that  $|D|$  is a 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. By induction on the number of irreducible branches of  $D_{red}$ , it's thus enough to show that  $H^1(\mathcal{O}_{D_{red}}) \simeq H^1(\mathcal{O}_{D'})$ . The short exact sequence

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

gives the long exact sequence in cohomology

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

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

By Corollary 2.4, there exists a unique line bundle  $\tilde{\mathcal{L}} \in \text{Pic}(X)$  so that  $\tilde{\mathcal{L}}|_{\partial X} \simeq \mathcal{L}|_{\partial X}$ . Let us consider the line bundle

$$\mathcal{L}_0 := \mathcal{L} \otimes \tilde{\mathcal{L}}|_D^{-1}.$$

Of course,  $\mathcal{L}$  lifts to  $X$  if and only if  $\mathcal{L}_0$  lifts. But  $\mathcal{L}_0|_{D_{red}}$  being trivial by construction,  $\mathcal{L}_0$  lifts to  $X$  if and only if  $\mathcal{L}_0 \simeq \mathcal{O}_D$ . Since the Chern class  $\delta_D(\mathcal{L}_0) = 0$  (by construction), we deduce from the diagram (6) that there exists  $\beta \in H^1(D, \mathcal{O}_D)$  with  $e(\beta) = \mathcal{L}_0$ . Moreover  $e$  is injective and finally

$$\mathcal{L} \text{ extends to } X \iff \mathcal{L}_0 \simeq \mathcal{O}_D \iff \beta = 0.$$

There remains to make explicit the condition  $\beta = 0$  in terms of the given data  $(D, \gamma)$ . We first use Čech cohomology. Suppose that  $\mathcal{L}_0$  is given by the 1-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

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

where  $\tilde{g}_{UV} \in \mathcal{O}_X^*(U \cap V)$  is some local lifting of  $g_{UV}$ . Since  $\delta_D(g) = 0$ , the classes  $h_{UV} \in \mathcal{O}_D(U \cap V)$  of  $\tilde{h}_{UV}$  define a 1-cocycle class  $\{h_{UV}\} \in H^1(D, \mathcal{O}_D)$  which represents  $\beta$  (this definition does not depend on the choice of 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*  $\delta : H^1(D, \mathcal{O}_D) \rightarrow H^2(X, \mathcal{O}_X(-D))$  while Serre Duality gives a non degenerate pairing

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

where  $\text{Tr}$  is the trace map [5]. We identify  $\mathcal{O}_X(-D)$  with the sheaf of functions vanishing on  $D$  and  $\Omega_X^2(D)$  with the sheaf of meromorphic 2-forms with polar locus bounded by  $D$ . The Serre pairing  $(\delta(\beta), \Psi)$  with  $\Psi \in H^0(X, \Omega_X^2(D))$  is represented by the 2-cocycle class

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

and  $\beta = 0$  if and only if

$$\text{Tr}(\zeta_\Psi) = 0 \quad \forall \Psi \in H^0(X, \Omega_X^2(D)).$$

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

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

and

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

where  $\theta$  is some test-form with appropriate bidegree and  $u = 0$  is a local equation for the polar divisor of  $\psi$  in a small neighborhood  $U$  of  $p$  (see [30] for instance). If  $\psi_1$  and  $\psi_2$  are two germs of meromorphic 1-forms at  $p \in X$  whose polar locus intersect properly at  $p$ , one can multiply the two residue currents  $\bar{\partial}[\psi_1]$  and  $\bar{\partial}[\psi_2]$ . If  $\theta$  is a test-function so that  $\theta \equiv 1$  in a neighborhood of  $p$ , we recover the usual Grothendieck residue introduced in formula (2) of Subsection 2.2

$$(8) \quad \langle \bar{\partial}[\psi_1] \wedge \bar{\partial}[\psi_2], \theta \rangle = \text{res}_p[\psi_1 \wedge \psi_2].$$

The Dolbeault resolution of  $\Omega_X^2$  is given by the exact complex of sheaves

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

This sequence breaks in the two short exact sequences

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

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

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

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

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

To make explicit  $T_\Psi$ , we need the following lemma.

**Lemma 2.5.** — 1. There exists a Cartier divisor  $\tilde{\gamma}$  on a small open neighborhood  $B$  of  $|D|$  which restricts to  $\gamma$  on  $D$ .

2. There exists a Cartier divisor  $E$  on  $X$  which restricts to  $\Gamma$  on  $D_{red}$  and there is an isomorphism  $\tilde{\mathcal{L}} \simeq \mathcal{O}_X(E)$ .

*Proof.* — 1. By means of a partition of unity, we can construct a  $\mathcal{C}^\infty$  function  $u$  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  $\gamma$ , and consider some local meromorphic liftings  $\tilde{f}_U$ . We can choose  $\mathcal{V}$  a sufficiently fine covering of  $B_\epsilon$  so that  $\tilde{f}_U \in \mathcal{O}_X(U)^*$  for  $U \cap |\Gamma| = \emptyset$  and so that  $U \cap V \cap |\Gamma| = \emptyset$  for distinct  $U, V \in \mathcal{V}$ . If  $U$  now intersects  $|\Gamma|$ , we can choose  $\epsilon' < \epsilon$  small enough so that  $\tilde{f}_U$  has no poles nor zeroes on  $U \cap V \cap B_{\epsilon'}$ . In such a way,  $\tilde{f}_U/\tilde{f}_V$  is invertible on  $U \cap V \cap B_{\epsilon'}$ , giving a Cartier divisor  $\tilde{\gamma}$  on  $B_{\epsilon'}$  which restricts to  $\gamma$  on  $D$ .

2. Let  $F$  be an effective divisor of  $X$  which intersects properly  $|D_{red}|$  and so that the line bundle  $\mathcal{F} = \mathcal{O}_X(F)$  is very ample. The isomorphisms

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

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

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

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

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

by the 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  $\Gamma$  on  $D_{red}$ . By construction  $\mathcal{O}_X(E)$  and  $\mathcal{L} = \mathcal{O}_D(\gamma)$  have the same restriction to  $D_{red} = \partial X$ , and Corollary 2.4 implies  $\tilde{\mathcal{L}} \simeq \mathcal{O}_X(E)$ .  $\square$

Let  $B, \tilde{\gamma}$ , and  $E$  be as in Lemma 2.5, with  $\mathcal{V}$  as the associated open covering of  $B$ . One keeps the notations of the proof of Lemma 2.5. Since  $\mathcal{O}_B(\tilde{\gamma}) \otimes \mathcal{O}_B(-E)$  restricts to  $\mathcal{L}_0$  on  $D$ , we can choose the liftings  $\tilde{g}_{UV}$  introduced after the proof of Corollary 2.4 to be  $\tilde{g}_{UV} = m_U/m_V$ , where  $m = \{m_U\}_{U \in \mathcal{V}}$  is the global meromorphic section of  $\mathcal{O}_B(\tilde{\gamma}) \otimes \mathcal{O}_B(-E)$  with Cartier divisor

$$\text{div}(m) = \tilde{\gamma} - E|_B$$

on  $B$ . For  $B$  small enough and for distincts  $U, V \in \mathcal{V}$ , one has  $m_U|_{U \cap V} \in \mathcal{O}_B^*(U \cap V)$  and there exists a logarithmic determination

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

Since  $\text{div}(m) \cdot D_{red} = 0$ , 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  $\Psi \in H^0(X, \Omega_X^2(D))$ . We can multiply a principal value current (or a residue current) with a residue current as soon as the supports of their singular sets have a proper intersection. Then, by the theorem of duality [30], we have here

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

so that the principal value currents

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

satisfy

$$(9) \quad (S_U - S_V) \bar{\partial}[\Psi_{U \cap V}] = [\log(\tilde{g}_{U \cap V})] \bar{\partial}[\Psi_{U \cap V}]$$

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  $\Psi$  is holomorphic outside  $|D|$ , we have  $T_U = 0$  when  $U \cap |D| = \emptyset$  and we can extend  $T_B$  by zero to a global current  $T$  on  $X$ . Using (9) and the definition of the coboundary maps, we check easily that  $T$  is by construction solution to

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

Let now  $\psi$  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

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

From (9) 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  $R_B$  and  $T'_B$  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, the 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  $\text{div}(m) = \tilde{\gamma} - E|_B$ , the Lelong-Poincaré equation gives equality

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

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

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

The analytic set  $B \cap \tilde{\gamma}$  is a disjoint union of analytic cycles  $\tilde{\gamma}_p = \{f_p = 0\}$ . If  $\psi_p$  is the germ of  $\psi$  at  $p$  in the chosen local coordinates, we obtain finally

$$\begin{aligned} \mathrm{Tr}(\zeta_\Psi) = \langle T, 1 \rangle &= \sum_{p \in |\Gamma|} \langle [\tilde{\gamma}_p] \wedge \bar{\partial}[\psi_p], 1 \rangle \\ &= \sum_{p \in |\Gamma|} \langle \bar{\partial}[df_p/f_p] \wedge \bar{\partial}[\psi_p], 1 \rangle \\ &= \sum_{p \in |\Gamma|} \mathrm{res}_p \left( \frac{df_p}{f_p} \wedge \psi_p \right) = \sum_{p \in |\Gamma|} \langle \gamma, \Psi \rangle_p, \end{aligned}$$

where the third and fourth equalities follow respectively from the Poincaré-Lelong equation and formula (8). Finally, (3) is equivalent to that  $\mathcal{L} = \mathcal{O}_D(\gamma)$  extends to  $\tilde{\mathcal{L}} \in \mathrm{Pic}(X)$ . Note that the complex number  $\sum_{p \in |\Gamma|} \langle \gamma, \Psi \rangle_p$  only depends on the line bundle  $\mathcal{O}_D(\gamma)$  and on  $\Psi$  by construction. If  $\mathcal{L}$  extends to  $\tilde{\mathcal{L}}$ , we can use the Serre vanishing theorem as in Lemma 2.5 (with  $(D, \gamma)$  instead of  $(D_{red}, \Gamma)$ ) and show that  $\tilde{\mathcal{L}} \simeq \mathcal{O}_X(E)$  for some Cartier divisor  $E$  on  $X$  which restricts to  $\gamma$  on  $D$ . The lifting bundle  $\tilde{\mathcal{L}}$  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 (3) hold, then  $\mathcal{L} \simeq \mathcal{O}_D(E)$  for some Cartier divisor  $E$  on  $X$ . By tensoring the structural sequence of  $D$  with  $\tilde{\mathcal{L}} = \mathcal{O}_X(E)$ , we obtain the short exact sequence

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

If  $\gamma$  is effective 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  $\gamma$  automatically lifts to  $\tilde{f} \in H^0(X, \mathcal{O}_X(E))$  and  $C := \mathrm{div}_0(\tilde{f})$  is an *effective* osculating divisor for  $(D, \gamma)$ . This ends the proof of Theorem 2.1.  $\square$

**2.5. An explicit formula in the toric case.** — We show now that we can make explicit the osculation conditions (3) 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. Preliminaries.* — Let us suppose now that  $X$  is a *toric* surface. The surface  $X$  is a disjoint union of a copy of the torus  $(\mathbb{C}^*)^2$  with some toric divisors  $D_0, \dots, D_{r+1}$  that are the Zariski closures of the 1-dimensional orbits of  $X$  under the torus action. Let us suppose moreover that  $X_0 \simeq \mathbb{C}^2$  is stable under the torus action. Then, we can order the  $D_i$ 's so that

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

is the boundary of  $X$  and  $D_0$  and  $D_{r+1}$  are the Zariski closures of the two 1-dimensional orbits contained in  $X_0$ .

Let  $\Sigma$  be the fan of  $X$ . We denote by  $\rho_i \in \Sigma$  the ray associated to the toric divisor  $D_i$ . Since  $X$  is smooth, its fan  $\Sigma$  is regular and we can order the  $D_i$ 's in such a way that the generators  $\eta_i$  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,

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

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

$$(10) \quad P_E = \{m \in \mathbb{R}^2, \langle m, \eta_i \rangle + e_i \geq 0, \ i = 0, \dots, r+1\},$$

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

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

and there is a natural isomorphism

$$(11) \quad H^0(X, \mathcal{O}_X(E)) \simeq \bigoplus_{m \in P_E \cap \mathbb{Z}^2} \mathbb{C} \cdot t^m,$$

where  $\mathcal{O}_X(E)$  is the sheaf of meromorphic functions with polar locus bounded by  $E$ . Similarly, the rational form  $\Psi_m$  defined by

$$\Psi_m|_{(\mathbb{C}^*)^2} = t^m \frac{dt_1 \wedge dt_2}{t_1 t_2}$$

has divisor  $\text{div}(\Psi_m) = \text{div}(t^m) - K_X$  where  $-K_X := D_0 + \dots + D_{r+1}$  is an anticanonical divisor, and there is equality

$$(12) \quad H^0(X, \Omega_X^2(E)) = \bigoplus_{m \in P_E + K_X \cap \mathbb{Z}^2} \mathbb{C} \cdot \Psi_m.$$

*2.5.2. Explicit osculating criteria.* — Let  $(D, \gamma)$  be an osculation data on  $\partial X$ . We note  $\Gamma = \gamma \cdot \partial X$  and  $\Gamma_i = \gamma \cdot D_i$ . By (12), the conditions (3) of Theorem 2.1 are equivalent to that

$$(13) \quad \sum_{p \in |\Gamma|} \langle \gamma, \Psi_m \rangle_p = 0 \quad \forall m \in P_{D+K_X} \cap \mathbb{Z}^2.$$

We give here an explicit formula for the residues  $\langle \gamma, \Psi_m \rangle_p$  when the following hypothesis holds:

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

In such a case, the germs  $\tilde{\gamma}_p$  are smooth, irreducible, and have transversal intersection with  $\partial X$ . For each  $p \in |\Gamma|$ , there is a unique component  $D_i$  containing  $p$  and we can choose the Weierstrass equation

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

for the germ  $\tilde{\gamma}_p$  in the affine coordinates of  $U_i$ . 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

**Proposition 2.6.** — *Suppose that  $\Gamma$  satisfies  $(H_1)$  and let  $m \in P_{D+K_X} \cap \mathbb{Z}^2$ . Then,*

$$(14) \quad \langle \gamma, \Psi_m \rangle_p = \frac{1}{(-\langle m, \eta_i \rangle)!} \frac{\partial^{-\langle m, \eta_i \rangle}}{\partial x_i^{-\langle m, \eta_i \rangle}} \left( \frac{\phi_p^{\langle m, \eta_{i+1} \rangle}}{\langle m, \eta_{i+1} \rangle} \right) (0)$$

for all  $p \in |\Gamma_i|$  and all  $i = 1, \dots, r$ . We use here conventions  $\phi_p^k/k := \log(\phi_p)$  for  $k = 0$  and  $\partial^a/\partial x^a(\phi_p^k/k) := 0$  for  $a < 0$ .

Since  $0 \notin P_{D+K_X}$ , equality  $\langle m, \eta_{i+1} \rangle = 0$  implies  $\langle m, \eta_i \rangle \neq 0$  and previous expression is well-defined since it depends only on the derivatives and logarithmic derivatives of  $\phi_p$  evaluated at 0 (recall that  $\phi_p(0) \neq 0$ ). Moreover,  $-\langle m, \eta_i \rangle \leq k_i$  and (14) only depends on  $\phi_p$  modulo  $(x_i^{k_i+1})$

**Example 2.7.** — (Wood's theorem). We keep the same hypothesis and notations of Example 2.2, now with an osculating order  $k \geq 2$ . Thus  $D = (k+1)L$ . Hypothesis  $(H_1)$  holds and by Proposition 2.6, there exists an osculating divisor for  $(D, \gamma)$  if and only if

$$(15) \quad \frac{\partial^{m_1+m_2}}{\partial x^{m_1+m_2}} \left( \sum_{p \in |\Gamma|} \frac{\phi_p^{m_1}}{m_1} \right) (0) = 0, \quad \forall m \in (\mathbb{N}^*)^2, m_1 + m_2 \leq k.$$

Since  $H^1(\mathcal{O}_{\mathbb{P}^2}(d-k-1)) = 0$  it follows that (15) is also sufficient for the existence of an osculating curve. When  $k \leq d+1$ , we recover a theorem of Wood, [35].

**2.5.3. Proof of Proposition 2.6.** — Let  $m \in P_{D+K_X}$ . In particular  $\langle m, \eta_0 \rangle \geq 1$  and we can suppose that  $m_2 \neq 0$ . The form  $\Psi_m$  is holomorphic in  $X_0$  and  $\Psi_m|_{X_0} = d(\psi_m|_{X_0})$  where  $\psi_m$  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

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

If  $\langle m, \eta_i \rangle > 0$ , the form  $\psi_m$  is holomorphic at  $p \in |\Gamma_i|$  and  $\text{res}_p(\frac{df_p}{f_p} \wedge \psi_m) = 0$ . Suppose now that  $\langle m, \eta_i \rangle \leq 0$ . The Cauchy integral representation for Grothendieck residues



of meromorphic forms does not depend on  $\epsilon$  for  $\epsilon_i$  small enough, thanks to the Stokes theorem. Thus, for sufficiently small  $\epsilon_i$ 's, we obtain

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

where the two last equalities are application of the Cauchy formula. In the same way, but simpler, we find

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

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

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

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 Proposition 2.6.  $\square$

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 2.1 and Proposition 2.6 to the classical 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 is comparable to a toric version of the Hensel lifting. It is in the spirit of the Abu Salem-Gao-Lauder algorithm [1], but uses vanishing-sums as in the Galligo-Rupperecht algorithm [13]. Our main contribution is that the underlying algorithmic complexity depends now on the Newton polytope  $N_f$  instead of the degree  $\deg(f)$ . We prove our main results Theorem 3.3 and Proposition 3.5 in Subsections 3.2 and 3.3. We describe the 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 by floating point computation with a given precision.

Suppose that  $f$  has the monomial expansion

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

We denote by  $N_f$  the Newton polytope of  $f$ , defined to be the convex hull of the exponents  $m \in \mathbb{N}^2$  for which  $c_m \neq 0$ . We recall that by a theorem of Ostrowski [28], we have relations

$$(16) \quad N_{f_1 f_2} = N_{f_1} + N_{f_2}$$

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

We assume that the following hypothesis holds.

$$(H_2) \quad \text{The Newton polytope of } f \text{ contains the origin.}$$

This equivalent to that  $f(0, 0) \neq 0$ .

**Remark 3.1.** — We can always find  $s \in \mathbb{Z}^2$  so that the Laurent polynomial  $ft^{-s}$  becomes a polynomial  $f' \in \mathbb{C}[u_1, u_2]$  with  $f'(0, 0) \neq 0$  after some *monomial* change of affine coordinates  $(t_1, t_2) \mapsto (u_1, u_2)$ . This transformation preserves the sparse structure of  $f$  so that hypothesis  $(H_2)$  is not restrictive for our purpose.

An *exterior facet* of  $N_f$  is a one-dimensional face  $F$  of  $N_f$  whose normal inward primitive vector has at least a negative coordinate. The associated normal ray of  $N_f$  is called an *exterior ray*. The associated *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  $\Sigma_f$  of  $\mathbb{R}^2$  whose rays are

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

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

clear for those contained in  $\partial X_f$  and the remaining torus fixed point of  $X_0$  does not belong to  $C_f$  by  $(H_2)$ .

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  $S := \text{Sing}(X_f)$  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  $\partial X$  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  $\rho_0, \dots, \rho_{r+1}$  the rays of the fan  $\Sigma$  of  $X$ , and by  $\eta_0, \dots, \eta_{r+1}$  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  $\pi(|D_i|) \subset S$ ).

**Lemma 3.2.** — *There is a unique effective divisor  $D$  linearly equivalent to  $C + \partial X$  with support  $|\partial X|$  and the polytope of the toric divisor  $D + K_X$  defined in (10) has lattice points*

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

*Proof.* — The polynomial  $f$  extends to a rational function on  $X$  whose polar divisor  $\text{div}_\infty(f)$  is supported by  $|\partial X|$ . Thus, the divisor

$$D := \text{div}_\infty(f) + \partial X$$

is effective, with support  $|\partial X|$ , and rationally equivalent to  $C + \partial X$ . If  $D'$  is another candidate, then  $D - D' = \text{div}(h)$  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  $D = D'$ . By using affine charts, we check easily that the polar divisor of  $f$  is equal to

$$\text{div}_\infty(f) = \sum_{i=1}^r k_i D_i, \quad k_i = - \min_{m \in N_f} \langle m, \eta_i \rangle.$$

By (11), it follows that  $N_f$  is contained in the polytope  $P_G$  of  $G = \text{div}_\infty(f)$  and intersects each face of  $P_G$ . Since the fan of  $X$  refines both normal fans of  $G$  and  $N_f$  (we use here hypothesis  $(H_2)$ ), it follows that  $P_G = N_f$ . Then, equality  $D + K_X = G - D_0 - D_{r+1}$  implies that

$$P_{D+K_X} = \{m \in P_G, \langle m, \eta_0 \rangle \geq 1, \langle m, \eta_{r+1} \rangle \geq 1\} = P_G \cap (\mathbb{N}^*)^2.$$

□

**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 from (16) 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 3.3.** — *Let  $f \in K[t_1, t_2]$  which satisfies  $(H_2)$ . Let  $\pi$ ,  $X$  and  $C$  be as before and denote by  $\gamma$  the restriction of  $C$  to the divisor  $D$  of Lemma 3.2. 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*

$$(17) \quad \deg(\gamma' \cdot D_i) = \text{Card}(Q^{(i)} \cap \mathbb{Z}^2) - 1, \quad i = 1, \dots, r$$

*and such that (3) holds for the osculation data  $(D, \gamma')$  on the boundary of  $X$ . The polynomial  $q$  can be recovered from  $\gamma'$ .*

Equation (17) means that the number of points (counted with appropriate multiplicity) in the support of  $\gamma'$  that belong to  $D_i$  has to be equal to the number of lattice points of the  $i$ -th edge of  $Q$  minus one (the so-called lattice length of the edge). When  $f$  satisfies hypothesis  $(H_1)$ , all the multiplicities are equal to one and the osculation criterions (3) can be tested efficiently thanks to Proposition 2.6. Note that  $Q^{(i)}$  is reduced to a point and  $\text{Card}(Q^{(i)} \cap \mathbb{Z}^2) - 1 = 0$  as soon as  $\rho_i$  is not an exterior ray of  $N_f$  so that (17) only involves the original fan  $\Sigma_f$  of  $f$ .

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

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

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  $\Sigma$  refines the normal fan of each polytope, we have equalities  $N_f = P_G$ ,  $Q = P_{G_Q}$  and  $P = P_{G_P}$  (see the proof of Lemma 3.2) 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  $|\mathcal{O}_X(G_Q)|$  of effective divisors rationally equivalent to  $G_Q$ . It defines a Cartier divisor  $\gamma' = C'|_D \leq C|_D = \gamma$  on  $D$ . Thus, conditions (3) hold for the osculation data  $(D, \gamma')$  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

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

for all  $i = 1, \dots, r$ . This shows necessity of conditions.

Suppose now that  $(D, \gamma')$  satisfies (17) and (3) and let  $F$  be an osculating divisor associated 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 2.4 of Subsection 2.4. Thus, if (3) and (17) hold for  $(D, \gamma')$ , one has an isomorphism  $\mathcal{O}_D(\gamma') \simeq \mathcal{O}_D(G_Q)$ . There remains to show that there exists in such a case an *effective* osculating divisor rationally equivalent to  $G_Q$ . 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  $\partial X$  is reduced and connected, the restriction map  $H^0(\mathcal{O}_X) \rightarrow H^0(\mathcal{O}_{\partial X})$  is an isomorphism and we deduce equality  $H^1(X, \mathcal{O}_X(-\partial X)) = 0$ . By Theorem 2.1, there thus exists  $C' \in |\mathcal{O}_X(G_Q)|$  with

$$(18) \quad C'_{|D_Q} = \gamma'_{|D_Q}.$$

Such a curve has proper intersection with the remaining toric divisors  $D_0$  and  $D_{r+1}$  (otherwise the support of  $\gamma'$  would contain a torus fixed point). We deduce that there exists a unique Cartier divisor  $\gamma_0$  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

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

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

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

implies that there exists  $C'' \in |\mathcal{O}_X(G_Q)|$  which restricts to  $\gamma_0$  on  $D + D_0 + D_{r+1}$ . A fortiori,  $C''$  restricts to  $\gamma'$  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

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

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

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

for all  $p$  in the support of  $D$ . Finally,

$$\deg(\mathcal{O}_X(C_0))|_C \geq \sum_{p \in |D|} \text{mult}_p(C_0, C) \geq \sum_{p \in |D|} \text{mult}_p(C_0, D) = \deg(\mathcal{O}_X(C_0))|_D.$$

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  $C$ . By (18), the component  $C_0$  appears in  $C'$  with a multiplicity smaller than in  $C$  and we deduce finally that  $C' \leq C$ , corresponding to an absolute factor  $q$  of  $f$  with Newton polytope  $Q$ .

Since  $G_Q - D_Q < 0$ , the restriction  $H^0(\mathcal{O}_X(G_Q)) \rightarrow H^0(\mathcal{O}_{D_Q}(G_Q))$  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  $\gamma'$ ).  $\square$

**Remark 3.4.** — If  $N_f$  does not contain the origin but only 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 can not conclude that  $N_q = Q$ .

**3.3. Computing the absolute factors of  $f$ .**— Suppose that  $\gamma' \leq \gamma$  satisfies conditions of Theorem 3.3 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  $[a] \in \mathbb{P}^{\text{Card}(Q \cap \mathbb{N}^2)-1}(\mathbb{C})$  of  $a = (a_m)_{m \in Q \cap \mathbb{N}^2}$ .

We denote by  $\Gamma' = \gamma' \cdot \partial X$  and by  $\Gamma'_i = \Gamma' \cdot D_i$ . Let us fix  $p \in |\Gamma'|$  and let  $i = i(p)$  be the unique index such that  $p \in |\Gamma'_i|$ . If  $f$  satisfies the hypothesis  $(H_1)$ , the germ of  $C$  at  $p$  has the Weirstrass equation

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

and we can define

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

for all integers  $u, v$  (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  $\text{Vol}(Q)$  the euclidean volume of  $Q$  in  $\mathbb{R}^2$ . We obtain the following

**Proposition 3.5.** — *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  $i = 1, \dots, r$ . The underlying linear system  $(S_{\gamma'})$  contains  $2 \text{Vol}(Q) + \deg(\Gamma')$  equations of  $\text{Card}(Q \cap \mathbb{Z}^2)$  unknowns and only depends on the restriction of  $\gamma'$  to the divisor  $G_Q + \partial X$ .

*Proof.* — We keep the notations of the proof of Theorem 3.3. By [11], the curve  $C'$  of  $q$  has affine polynomial equation  $q_i = 0$  in the chart  $U_i = \text{Spec } \mathbb{C}[x_i, y_i]$ , where

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

Let  $p \in |\Gamma'_i|$ . Since the germ of  $C'$  at  $p$  is contained in that of  $C$  it follows that

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

It's easy to show that the  $k^{\text{th}}$ -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  $(S_{\gamma'})$ .

If  $\tilde{a} = (\tilde{a}_m)_{m \in Q \cap \mathbb{Z}^2}$  is another non trivial solution of  $(S_{\gamma'})$ , the polynomial  $\tilde{q}(t) = \sum_{m \in Q \cap \mathbb{Z}^2} \tilde{a}_m t^m$  satisfies

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

for all  $p \in |\Gamma'_i|$ , all  $0 \leq k \leq e_i$  and all  $i = 1, \dots, r$ . By the duality theorem, this forces the germ of  $\tilde{q}_i$  at  $p$  to belong to the ideal  $(y_i - \phi_p(x_i), x_i^{e_i+1})$ . It follows that the curve  $\tilde{C} \subset X$  of  $\tilde{q}$  satisfies

$$\tilde{C}|_{\sum (e_i+1)D_i} \geq C'|_{\sum (e_i+1)D_i}.$$

Since  $N_{\tilde{q}} \subset Q = N_q$ , it follows that  $\deg(\tilde{C} \cdot D_i) \leq \deg(C' \cdot D_i)$  for all  $i$ . Combined with previous inequality, this forces equality

$$C'|_{\sum (e_i+1)D_i} = \tilde{C}|_{\sum (e_i+1)D_i}.$$

We have chosen the  $e_i$ 's in order to that

$$\sum_{i=1}^r (e_i + 1)D_i = G_Q + \partial X,$$

and both curves  $C'$  and  $\tilde{C}$  belong to the linear system  $|\mathcal{O}_X(G_Q)|$ . The restriction map  $H^0(X, \mathcal{O}_X(G_Q)) \rightarrow H^0(X, \mathcal{O}_{G_Q+\partial X}(G_Q))$  being injective, the previous equality forces  $C' = \tilde{C}$ . It follows that  $\tilde{q} = cq$  for some  $c \in \mathbb{C}^*$  and  $[a] = [\tilde{a}]$ .

By construction, the linear system  $(S_{\gamma'})$  only depends on the restriction of  $\gamma'$  to the divisor  $G_Q + \partial X < G + \partial X = D$ . It contains precisely

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

equations and  $\deg(C' \cdot G_Q) = \deg(C' \cdot C') = 2 \text{Vol}(Q)$  unknowns (see [14] for instance).  $\square$

**Remark 3.6.** — Each linear equation in Proposition 3.5 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  $i = 1, \dots, r$  the linear subsystem

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

It has  $\text{Card}(Q^{(i)} \cap \mathbb{Z}^2) - 1$  equations with  $\text{Card}(Q^{(i)} \cap \mathbb{Z}^2)$  unknowns and permits to determine the coefficients of the  $i^{\text{th}}$  exterior facet polynomial 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  $\{a_m, \langle m, \eta_i \rangle + e_i = k\}$ . In general, there are no non trivial solutions to  $(S_{\gamma'})$ . The vector subspace of solutions has dimension 1 precisely when  $\gamma'$  obeys to the osculation conditions (3).

**3.4. A sparse vanishing-sums algorithm.** — We describe here a sparse vanishing-sums algorithm associated to Theorem 3.3 and Proposition 3.5. When we say compute, we mean compute by using floating point computation with a given precision. When we say test a vanishing-sum, we mean test that a sum is  $\leq \epsilon$  for an arbitrary small  $\epsilon > 0$ .

*Input:* A polynomial  $f \in K[t_1, t_2]$  which satisfies  $f(0, 0) \neq 0$  and with reduced 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  $N_f$  has no non trivial Minkowski summands,  $f$  is irreducible and the algorithm stops. Otherwise go to step 2.

*Step 2.* Compute the fan of  $X$ . Compute the canonical regular fan  $\Sigma$  that refines  $\Sigma_f$  by using an Euclidean algorithm, or by computing some Hirzebruch-Jung continued fraction (see [14]).



*Step 3. Compute the osculating data  $(D, \gamma)$ .* By Lemma 3.2, 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  $\gamma$  on  $D$  is obtained by computing the family of implicit functions  $\{\phi_p, p \in |\Gamma_i|\}$  up to order  $k_i$ , for  $i = 1, \dots, r$ . Note that  $\Gamma_i = 0$  when  $\rho_i$  is not an exterior ray of  $N_f$ .

*Step 4. Compute the Newton polytopes of the absolute irreducible factors.* Proposition 3.5 combined with Theorem 3.3 gives an efficient way to compute the decompositions

$$\gamma = \gamma_1 + \dots + \gamma_s, \quad N_f = Q_1 + \dots + Q_s$$

of  $\gamma$  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 3.5. The coefficients of the linear systems  $(S_{\gamma_i})$ ,  $i = 1, \dots, s$  are obtained from the residues  $\langle \gamma, \Psi_m \rangle_p$ ,  $m \in Q_i \cap (\mathbb{N}^*)^2$  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-test, up to obtain the adequate decomposition of  $N_f$ . Finally, we compute the factors by solving some linear systems. Roughly speaking, we obtain here a toric version of the Hensel lifting (see Remark 3.6). A comparable algorithm has been obtained by Abu Salem-Gao-Lauder in [1], by using combinatorial tools.

If we can decide formally if the sum underlying the osculation criterions (13) vanishes, there is no chance of failure in step 4 and the algorithm is deterministic. If we test the osculating criterions (13) 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].

As in [13] and [12], floating point computation and numerical approximation *a priori* do not allow to decide in a deterministic way if the sum (13) is equal to 0, but one rather decide if it is smaller than a given small  $\epsilon$ . 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 of 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.** — We compare here our algorithm with those of Galligo-Rupprecht [13], Elkadi-Galligo-Weimann [12] and Weimann [33].

*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  $\mathbb{C}\{t_1\}[t_2]$  modulo  $(t_1^3)$ . They detect the factors of  $f$  with probability one by testing the Reiss relation (4) on subfamilies  $\mathcal{F} \subset \{\phi_i, i = 1, \dots, d\}$ . Then they lift and compute the candidate factors by using Hensel lemma. Let us compare with our approach.

*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 (17), 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 have the following improvement:

**Proposition 3.7.** — *Suppose that  $f$  is irreducible over  $K$  and satisfies hypothesis  $(H_1)$  and  $(H_2)$ . Let  $d = \deg(f)$ . Then*

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

*with equality*

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

*where Conv designs the convex hull.*

*Proof.* — Let  $n$  be the biggest integer so that  $N_f = nQ_0$  for a lattice polytope  $Q_0$ . Thus  $d = nl$  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  $\mathcal{M}(f) \leq 2^d$ . Equality  $\mathcal{M}(f) = 2^d$  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 lengths of the exterior facets of  $Q_0$ . Then, restrictions (17) 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

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

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

$$l_f = nl_1 + \dots + nl_t$$

of the lattice lengths of the exterior facets of  $N_f$  is smaller or equal to  $d = \deg(f)$ . Moreover, we can convince that there is equality  $l_f = d$  if and only if the normal fan  $\Sigma_f$  of  $N_f$  is regular. This is of course exceptional, and  $l_f \ll d$  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  $N_f = \text{Conv}\{(0, 0), (d, 0), (0, d)\}$ .  $\square$

Note that there are fast factorization algorithms over a number field  $K$  (see [4], [26]). The following example illustrates Proposition 3.7.

**Example 3.8.** — Suppose that  $f$  is irreducible over  $K$  and that  $N_f = nQ_0$ , where  $Q_0$  is the “undivisible” lattice polytope

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

with  $a \geq 2$  and  $n$  prime. The lattice lengths 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, it 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 grows exponentially with  $a$ .

The asymptotic estimation of  $\mathcal{N}(f)$  for a “generic polytope”<sup>(1)</sup>  $N_f$  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 3.2 and Theorem 3.3, the maximal number of vanishing-sums to test is equal to

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

<sup>(1)</sup>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 (13) 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.

*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  $l_1, \dots, l_t$  than one univariate polynomial of total degree  $d \geq l_1 + \dots + l_t$ . Thus, the computation of  $C \cdot \partial X$  is faster than with a generic line as soon as  $\mathcal{N}(f) < \mathcal{M}(f)$ .

*The lifting step.* Although we need to compute a reduced number of implicit functions, we need *in general* a bigger precision on the  $\phi_p$ 's than the upper bound  $\deg(f)$  precision required with the classical Hensel lifting. In Example 3.8, we need for instance to compute the  $\phi_p$ 's up to order  $na^2 \gg 2na = \deg(f)$ . Morally, the more the recombination number is reduced, the more the required precision on the  $\phi_p$ 's increases. Thus, we should be very careful when comparing algorithmic complexity. Nevertheless, we gain on both sides in the important case of a polynomial of bidegree  $(a, b)$ . Formulas (13) and (14) 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 propose an algorithm with the recombination number  $\mathcal{N}(f)$  by using the interpolation criterions obtained in [31]. Their approach necessitates 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 Newton polytope  $P$  and  $\epsilon$  is a small positive real number. When  $\epsilon$  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. As in the GR-algorithm, the generic choice of  $p$  in the EGW-algorithm 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. Roughly speaking, Theorem 3.3 corresponds to the limit case  $\epsilon = 0$  and permits to avoid the delicate problem of the “small enough  $\epsilon$ ” choice and of the asymptotic distribution lecture. We compute only  $\deg(C \cdot \partial X) \ll \deg(C \cdot L)$  implicit functions (but with a precision  $\gg 2$ ) and we detect the absolute decomposition of  $f$  deterministically.

*3.5.3. Comparison with Weimann algorithm [33].* — Our algorithm described in Subsection 3.4 has been improved later by the author who obtained a deterministic algorithm that factors rational bivariate polynomials in low-degree polynomial time in the volume of the Newton polytope. Nevertheless, although the algorithm described in Subsection 3.4 has an exponential complexity, this complexity depends both on the number of Minkowski summands and on the number of lattice points on the edges of the polytope of  $f$ , these two numbers being quite small for a sparse polynomial

(Subsection 3.5.1). On another hand, we use here a lifting precision  $D \simeq C + \partial X$  ( $= \deg(f) + 1$  in the dense case) that is almost two times smaller than the lifting precision  $D \simeq 2C$  ( $= 2 \deg(f)$  in the dense case) required in [33]. Thus, in some particular cases, the exponential time algorithm we present here might be faster than the polynomial time approach obtained in [33]. Moreover, recent works of the author tend to show that the exponential complexity approach developed here generalizes well to the singular case (see Subsection 3.6), although the polynomial time algorithm of [33] does not, due to some problem of vanishing cohomology.

**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 multiple roots). 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 (14).

Nevertheless, there exists in such a case a (non toric) smooth completion  $\tilde{X}$  of  $\mathbb{C}^2$  obtained from  $X$  by a series of blow-ups, and so that the proper transform  $\tilde{C} \subset \tilde{X}$  of  $C$  has a transversal intersection with the boundary of  $\tilde{X}$ . By choosing an effective divisor  $\tilde{D}$  supported on  $\partial\tilde{X}$  and with sufficiently big multiplicities, we can then use Theorem 2.1 efficiently to decompose  $\tilde{C}$  and to recover the absolute factorization of  $f$ . The added exceptional divisors give new restrictions on the possible choices of  $\tilde{\gamma}' < \tilde{\gamma}$  (where  $\tilde{\gamma} = \tilde{C}|_{\tilde{D}}$ ) and the presence of singularities of  $C$  along  $\partial X$  finally turns out to be an opportunity to reduce the recombination number. This will be explored in a further work.

**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. 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 osculation criterions in an appropriate toric resolution  $X$  permit to use this sparse information. Moreover, Theorem 2.1 permits in theory to consider the case when  $C$  has singularities along the boundary of  $X$ .

## 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*, Manuscript (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 problem*, 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., Vol. 44, no. 9 (2009), pp. 1194-1211.
- [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. 89-124.
- [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. 128 (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. Lovz, *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] M. Weimann, *A lifting and recombination algorithm for rational factorization of sparse polynomials*, J. of Complexity Vol. 26, no 6 (2010), pp. 608-628.
- [34] J.A. Wood, *A simple criterion for an analytic hypersurface to be algebraic*, Duke Math. J. 51 (1984), pp. 235-237.
- [35] J.A. Wood, *Osculation by Algebraic Hypersurfaces*, J. Differential Geometry 18 (1983), pp. 563-573.

---

MARTIN WEIMANN, Departament Algebra i Geometria, Facultat de Matemàtiques, Universitat  
Barcelona Gran via 585, 08007 Barcelona. • *E-mail* : [weimann23@gmail.com](mailto:weimann23@gmail.com)  
*Url* : [adresse WWW](http://adresse WWW)