A lifting and recombination algorithm for rational factorization of sparse polynomials

Martin Weimann

A LIFTING AND RECOMBINATION ALGORITHM FOR RATIONAL FACTORIZATION OF SPARSE POLYNOMIALS

MARTIN WEIMANN

Abstract. We propose a new lifting and recombination scheme for rational bivariate polynomial factorization that takes advantage of the Newton polytope geometry. We obtain a deterministic algorithm that can be seen as a sparse version of an algorithm of Lecerf, with now a polynomial complexity in the volume of the Newton polytope. We adopt a geometrical point of view, the main tool being derived from some algebraic osculation criterions in toric varieties.

1. Introduction and main results

This article is devoted to develop an algorithm for factoring a bivariate polynomial f over a number field $\mathbb{K}$ by taking advantage of the geometry of its Newton polytope. Geometrically, this corresponds to decomposing the curve defined by f in a suitable toric surface X. We will thus talk about a toric factorization algorithm. The usual case of dense polynomials corresponds to the classical projective completion $X = \mathbb{P}^2$ of the complex plane. Our approach is based on algebraic osculation. The central idea is that we can recover the decomposition of the curve $C \subset X$ defined by f from its restriction to a suitable toric Cartier divisor D. In a previous work [28], we developed a similar method based on vanishing-sums criterions and obtained an exponential complexity toric factorization algorithm. In contrast, we use here a lifting and recombination model based on a vector space basis computation which conduces to a polynomial complexity algorithm. Our method can be regarded as a toric version of the algorithms developed by Lecerf [18], [19] and by Chèze and Lecerf [8] for dense polynomials. Let us expose our main results.

Main results. Let $\mathbb{K}$ be a number field and let $f \in \mathbb{K}[t_1, t_2]$ be a bivariate polynomial. Suppose that f has monomial expansion

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

where $m = (m_1, m_2)$ and $t^m = t_1^{m_1} t_2^{m_2}$. The Newton polytope N_f of f is the convex hull of the exponents m for which c_m is not zero. An exterior facet F of N_f is a one-dimensional face whose primitive inward normal vector has at least one negative coordinate. The associated facet polynomial of f is the univariate polynomial obtained from $f_F = \sum_{m \in F} c_m t^m$ after a suitable monomial change of coordinates. In all of the sequel, we assume the following hypothesis

- (H_1) *The polytope N_f contains the points $(0,0)$, $(1,0)$, $(0,1)$.*
- (H_2) *The exterior facet polynomials of f are squarefree.*

We denote by ω the matrix multiplication exponent. It's well known [15] that $2 < \omega < 2.37$. In all of the sequel, rational factorization means irreducible factorization over $\mathbb{K}$. Our main result is the following

Theorem 1. *There is a deterministic algorithm that, given $f \in \mathbb{K}[t_1, t_2]$ which satisfies (H_1) and (H_2), and given the rational factorization of the exterior facet polynomials of f, computes the rational factorization of f with $\mathcal{O}(\mathrm{Vol}(N_f)^\omega)$ arithmetic operations in $\mathbb{K}$.*

In some cases, our complexity improves that of the fastest actual algorithms which would treat f as a dense polynomial. In any case, the degree sum of the exterior facet polynomials of f is smaller than the total degree of f so that the unavoidable univariate factorization step is faster using the toric approach. The gain might be considerable as illustrates the following example.

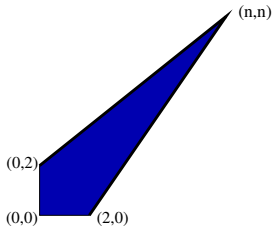

FIGURE 1. Each exterior facet contains at most 3 lattice points and $\mathrm{Vol}(N_f) = \mathcal{O}(n)$. Our algorithm will perform two univariate factorizations in degree at most 2 and $\mathcal{O}(n^\omega)$ operations while the fast algorithm of Lecerf [19] will perform a change of coordinates, one univariate factorization in degree $2n$ and $\mathcal{O}(n^{\omega+1})$ operations.

Let us explain the main tools for proving Theorem 1. We strongly suggest to the reader to follow our method and results on the concrete example developed in Subsection 3.5, p.19.

By the hypothesis (H_1), we can consider a complete *regular* fan Σ that refines the normal fan Σ_f of N_f and that contains the regular 2-dimensional cone generated by the canonical basis of $\mathbb{R}^2$. Such a fan determines a smooth complete toric surface $X = X_\Sigma$ and a torus-equivariant embedding of the affine plane $\mathbb{C}^2 = \mathrm{Spec}\,\mathbb{C}[t_1, t_2]$ into X. The rational factorization of f correspond to the decomposition over $\mathbb{K}$ of the Zariski closure $C \subset X$ of the affine curve defined by f. The geometry of N_f is related to the intersection of C with the boundary divisor

$$\partial X := X \setminus \mathbb{C}^2$$

of the toric completion X, and we want to use this information.

Let $\mathrm{Div}(X)$ be the group of Cartier divisors of X. We definitively fix $D \in \mathrm{Div}(X)$ effective with support $|D| = |\partial X|$. For convenience, we identify D with the induced subscheme $(|D|, \mathcal{O}_D)$ of X and we denote by $\mathrm{Div}(D)$ the group of Cartier divisors of D. The inclusion morphism $i : D \to X$ induces a restriction map i^* on the

subgroup of divisors of X who intersects D properly. In particular, we can consider the restriction

$$\gamma_C := i^*(C) \in \mathrm{Div}(D)$$

of C to D. The main idea is that for D chosen with sufficiently big multiplicities, we can recover both the rational and the absolute (over $\bar{\mathbb{K}}$) factorization of f from γ_C.

The irreducible decomposition of $C \cap \partial X$ over $\mathbb{K}$ is indexed by the set $\mathcal{P}$ of the monic irreducible rational factors of all of the exterior facet polynomials of f and we decompose γ_C accordingly as

$$\gamma_C = \sum_{P \in \mathcal{P}} \gamma_P,$$

where γ_P corresponds to lifting P to a local factor of f modulo a local equation of D (see Subsections 3.1 and 3.5). The recombination problem consists in computing the partition of $\mathcal{P}$ that corresponds to the rational decomposition of C. To this aim, we introduce the free $\mathbb{Z}$-module

$$V_{\mathbb{Z}} := \Big\{ \sum_{P \in \mathcal{P}} \mu_P \gamma_P,\ \mu_P \in \mathbb{Z} \Big\} \subset \mathrm{Div}(D),$$

and the submodule

$$V_{\mathbb{Z}}(D) := \{\gamma \in V_{\mathbb{Z}};\ \exists\, E \in \mathrm{Div}(X),\ i^*(E) = \gamma\}$$

of divisors of D that extend to X. We set $V := V_{\mathbb{Z}} \otimes \mathbb{K}$ and $V(D) := V_{\mathbb{Z}}(D) \otimes \mathbb{K}$. By construction, the irreducible rational decomposition $C = C_1 \cup \cdots \cup C_s$ of C generates a vector subspace

$$\langle \gamma_1, \ldots, \gamma_s \rangle \subset V(D)$$

where $\gamma_j := i^*(C_j)$. By the hypothesis (H_2), the γ_j's are pairwise orthogonal in the basis $(\gamma_P)_{P \in \mathcal{P}}$ of V and so $\dim V(D) \geq s$. The following theorem asserts that equality holds for D big enough. We say that a basis $(\nu_1, \ldots, \nu_n)$ of $V(D) \subset V$ is a *reduced echelon basis* of $V(D)$ if the matrix with j^{th} row ν_j is in its reduced echelon form in the canonical basis of the input space V (see [24]). Such a basis exists and is unique. We obtain the following

Theorem 2. *Let* $\mathrm{div}_\infty(f)$ *be the polar divisor of the rational function of* X *induced by* f*. If the inequality*

$$D \geq 2\,\mathrm{div}_\infty(f)$$

holds, then $(\gamma_1, \ldots, \gamma_s)$ *is the reduced echelon basis of* $V(D)$*.*

The proof consists in associating to $\gamma \in V_{\mathbb{Z}}(D)$ a rational 1-form with polar divisor controled by C. For D big enough, that form is closed and a theorem of Ruppert [23] combined with a Galois theory argument permits to conclude that γ is $\mathbb{Z}$-combination of the γ_i's. There are examples in the dense case that show that the precision $D = 2\,\mathrm{div}_\infty(f)$ in Theorem 2 is asymptotically sharp (see [19]).

In order to apply Theorem 2 to the factorization problem, we need to determine an explicit system of equations that gives the vector subspace $V(D) \subset V$. To this

aim, we use a theorem of the author that characterizes the lifting property. We show in [28] that there exists a morphism

$$\Psi : \mathrm{Div}(D) \otimes \mathbb{C} \to H^0(X, \Omega^2_X(D))^\vee$$

so that $\gamma \in \mathrm{Div}(D)$ extends to X if and only if $\Psi(\gamma) = 0$. Roughly speaking, the linear form $\Psi(\gamma)$ sends a rational form $\omega \in H^0(X, \Omega^2_X(D))$ to the sum of residues of a primitive of ω along a local analytic lifting curve of γ. In some sense, this result can be regarded as a converse to the classical residue theorem, we refer to [28] for details. This permits to prove the following

Theorem 3. *Suppose that D satisfies the hypothesis of Theorem 2. Then,*

$$V(D) = \ker(A)$$

for some explicit matrix $A = (a_{P,m})_{P\in\mathcal{P},m\in M}$ with coefficients in $\mathbb{K}$, where M is the set of interior lattice points of the polytope $2N_f$.

So we can solve the recombination problem with linear algebra over $\mathbb{K}$. Then, we compute the rational factors of f by solving systems of affine equations. We finally obtain a deterministic polynomial complexity algorithm for rational toric factorization of bivariate polynomials. We describe briefly the main steps of the algorithm. The given complexities are obtained in Corollaries 1 and 2 in Section 3. As in [15], we use the notation $\widetilde{\mathcal{O}}$ for the soft complexity.

Toric Factorization Algorithm

Input: $f \in \mathbb{K}[t_1, t_2]$ satisfying hypothesis (H_1) and (H_2).

Output: The irreducible rational factors of f.

Step 0: Univariate factorization. Compute the set $\mathcal{P}$ of irreducible rational factors of the exterior facet polynomials of f.

Step 1: Lifting. This is the γ_P's computation step. For each $P \in \mathcal{P}$, compute the associated local factor of f modulo the local equation of $D = 2\,\mathrm{div}_\infty(f)$. This step has complexity $\widetilde{\mathcal{O}}(\mathrm{Vol}(N_f)^2)$.

Step 2: Recombination.

a) Build the matrix A of Theorem 2. This step has complexity $\widetilde{\mathcal{O}}(\mathrm{Vol}(N_f)^2)$.

b) Compute the reduced echelon basis associated to A. This step has complexity $\mathcal{O}(\mathrm{Vol}(N_f)\,\mathrm{Card}(\mathcal{P})^{\omega-1})$.

Step 3: Factors computation. Solve some affine systems of linear equations over $\mathbb{K}$ to recover the rational factors of f. This step has complexity $\mathcal{O}(\mathrm{Vol}(N_f)^\omega)$.

A great advantage of our algorithm is that it replaces the usual univariate factorization in degree $d = \deg(f)$ by the factorization of the exterior facet polynomials of f : their degree sum is at most d, and much smaller in many significant cases. Thus both the number of unknowns and equations in the recombination process decrease too and the basis computation step 2 *b*) is faster than in [19]. Steps 1 and 2 *a*) rely on classical modular algorithms (Newton iteration, modular multiplication) whose complexity analysis is delicate due to the sparseness of f. This partially explains that our lifting complexity does not reach the soft complexity $\widetilde{\mathcal{O}}(d^2)$ obtained in

[19] for dense polynomials. Step 3 has the highest cost of the algorithm because in the general sparse case we have to use linear algebra instead of the fast multiplication or partial fraction decomposition methods that are used for dense polynomials ([14], [18], [8]). Finally, let us mention that the algorithm developed by Lecerf [18] in the bidegree case suggests that it is possible to reduce both the number of facet factorizations and the lifting precision. We refer to Section 4 for further comments.

Related results. Classical results about polynomial factorization can be found in [15]. For more recent advances, we refer the reader to the introduction of [8] (and to the complete list of references therein) that gives a large and comprehensive overview of the current algorithms for factorization of polynomials. We only discuss here the most related results.

Using linear algebra. Factoring multivariate polynomials by means of linear algebra has been made possible by the powerful irreducibility criterion of Ruppert [23]. This is the so-called logarithmic derivative method, that relates the basis computation of the vector space of closed rational 1-forms with some appropriate polar divisor. This point of view has been developed by Gao in [14], who combined the logarithmic derivative method with the Rothstein-Trager algorithm for absolute partial fraction decomposition ([15], Theorem 2.8). Finally, as pointed out in the introduction, Lecerf [19], [18] and Chèze-Lecerf [8] recently developed very efficient hybrid algorithms for rational and absolute factorization, by combining Gao's approach with a lifting and recombination scheme. This is the point of view we follow here.

Using Newton polytopes. Factoring polynomials by taking into account the Newton polytope is an active area of research. In [11], M. Elkadi, A. Galligo and the author use some probabilistic interpolation criterions [27], by replacing the divisor D with a generic ample curve "close to the boundary". In [28], the author looks for the *effective* decompositions of γ_C that may be lifted to X. By taking into account natural degree conditions imposed by the Minkowski-sums decompositions of N_f, there appears supplementary vanishing cohomology properties of the osculating divisors that permit to use the smaller precision $D = \mathrm{div}_\infty(f) + \partial X$ (see also [18] for a similar comparison in the dense case). In return, it gives a problem of partitions of $V(D) \cap \{0,1\}^{\mathcal{P}}$ that has exponential complexity in the worst case (see Subsection 3.6). A comparable algorithm is obtained in [1], where the authors use a more combinatorial approach. In [3], the authors show that the low degree factors of f can be computed in polynomial time with respect to the fewnomial encoding of f.

Organization. We prove Theorem 2 in the next Section 2. In Section 3, we develop a toric factorization algorithm, we prove Theorem 1 and we develop an example. In Section 4, we compare our method with the most related dense and toric algorithms and we discuss some possible improvements. We conclude in Section 5.

2. Proof of Theorem 2

We follow the notations of the introduction. We saw that the rational decomposition $C = C_1 \cup \cdots \cup C_s$ of C generates a vector subspace $\langle \gamma_1, \ldots, \gamma_s \rangle \subset V(D)$ and we want to show that the opposite inclusion holds when $D \geq 2\,\mathrm{div}_\infty(f)$. The strategy

consists in associating to $\gamma \in V_{\mathbb{Z}}(D)$ a closed rational 1-form ω on X whose polar divisor is controled by C. A theorem of Ruppert [23] implies that ω is a $\mathbb{C}$-linear combination of the logarithmic derivatives of the absolute factors of f. Finally, we conclude by Galois theory that γ is $\mathbb{Z}$-combination of the γ_j's.

We need first two preliminaries lemmas that clear up the behaviour of restriction with respect to derivation. The remaining part of the proof will follow in Subsection 2.2. If not specified, all schemes are considered over $\mathbb{C}$.

2.1. **Notations and preliminaries lemmas.** We denote by I_D the ideal sheaf of D and by $\mathcal{O}_D$ its structural sheaf. The structural sequence of D is

$$0 \to I_D \to \mathcal{O}_X \stackrel{i^*}{\to} \mathcal{O}_D \to 0, \tag{1}$$

where the restriction map i^* is induced by the inclusion $i : D \to X$. We denote by $\mathcal{O}_X(D)$ the sheaf of rational functions with polar divisor bounded by D, by Ω^q_X the sheaf of regular q-forms and we let $\Omega^q_X(D) := \Omega^q_X \otimes \mathcal{O}_X(D)$.

We say that $B \in \mathrm{Div}(X)$ is a normal crossing divisor if it has local equation $x_1 \cdots x_r = 0$ where the x_i's form part of a local system of coordinates $(x_1, \ldots, x_n)$ of X (so $n = 2$ in our case). For such a B, we introduce the sheaf $\Omega^q_X(\log B)$ of rational q-forms with logarithmic poles along B. By definition, $\phi \in \Omega^q_X(\log B)$ if and only if both $h\phi$ and $hd\phi$ are regular for some local equation $h = 0$ of B. It is well known that $\Omega^q_X(\log B)$ is a locally free sheaf of $\mathcal{O}_X$-module [25].

The following lemma clears up the behaviour of the restriction morphism with derivation.

Lemma 1. *Let B, D as before, with $|D| \subset |B|$. Let F be an effective divisor which intersects D properly. The differential d induces a commutative diagram*

$$\begin{array}{ccc} \Omega^1_X(\log B) \otimes \mathcal{O}_X(F) & \stackrel{d}{\to} & \Omega^2_X(B) \otimes \mathcal{O}_X(2F) \\ \downarrow i^* & & \downarrow i^* \\ \Omega^1_X(\log B) \otimes \mathcal{O}_D(F) & \stackrel{d_D}{\to} & \Omega^2_X(B) \otimes \mathcal{O}_D(2F). \end{array}$$

Proof. We show Lemma 1 for an arbitrary smooth complete variety X of dimension n. Since B is normal crossing, it has local equation $x_1 \cdots x_r = 0$ where the x_i's form part of a local system of coordinates $(x_1, \ldots, x_n)$ of X. The sheaf $\Omega^1_X(\log B)$ is a locally free sheaf of $\mathcal{O}_X$-modules and a germ $\phi \in \Omega^1_X(\log B) \otimes \mathcal{O}_X(F)$ has a unique representation

$$\phi = h_1 dx_1/x_1 + \cdots + h_r dx_r/x_r + h_{r+1} dx_{r+1} + \cdots + h_n dx_n$$

for some $h_i \in \mathcal{O}_X(F)$ (see [25], p. 186). It is clear that dh_i has its polar divisor bounded by $2F$. We deduce that

$$d\phi = dh_1 \wedge dx_1/x_1 + \cdots + dh_n \wedge dx_n$$

belongs to $\Omega^2_X(B + 2F)$ and the upper row is well-defined. In order to show that d_D is well-defined, we need to show that

$$\phi \in \Omega^1_X(B + F) \otimes I_D \Longrightarrow d\phi \in \Omega^2_X(B + 2F) \otimes I_D.$$

Since D is supported on $|B|$, it has local equation $x^k := x_1^{k_1} \cdots x_r^{k_r}$ for some $k_i \in \mathbb{N}$. Thus if $\phi \in \Omega^1_X(B+F) \otimes I_D$, we have $h_i = x^k h'_i$ for some $h'_i \in \mathcal{O}_X(F)$ and

$$\frac{dh_i}{x^k} \wedge \frac{dx_i}{x_i} = h'_i \sum_{j=1}^{r} k_j \frac{dx_j}{x_j} \wedge \frac{dx_i}{x_i} + dh'_i \wedge \frac{dx_i}{x_i}$$

belongs to $\Omega^2_X(B+2F)$ for all $i = 1, \ldots, r$. In the same way, it is easy to check that $dh_i \wedge dx_i/x^k \in \Omega^2_X(B+2F)$ for $i > r$. Multiplying by x^k, we obtain that $d\phi \in \Omega^2_X(B+2F) \otimes I_D$. □

We now pay attention to the behaviour of the restriction map with logarithmic derivation. We denote by $\mathcal{M}_{X,D}$ the sheaf of rational functions whose polar locus intersects D properly. We have an exact sequence

$$0 \to I_D\mathcal{M}_{X,D} \to \mathcal{M}_{X,D} \xrightarrow{i^*} \mathcal{M}_D \to 0, \tag{2}$$

where $\mathcal{M}_D := \mathcal{M}_{X,D} \otimes \mathcal{O}_D$ is the sheaf of rational sections of $\mathcal{O}_D$. The multiplicative version of (2) is

$$0 \to 1 + I_D\mathcal{M}_{X,D} \to \mathcal{M}^*_{X,D} \xrightarrow{i^*} \mathcal{M}^*_D \to 0, \tag{3}$$

where * stands for the multiplicative sheaves of units. On the other hand, the logarithmic derivative $d\log(h) := dh/h$ induces the natural morphisms

$$d\log : \mathcal{M}^*_{X,D} \to \Omega^1_X \otimes \mathcal{M}_{X,D} \quad \text{and} \quad d\log : \mathcal{O}^*_X \to \Omega^1_X \tag{4}$$

of sheaves of abelian groups. We have the following

Lemma 2. *Let B, D as before and suppose that $|D| \subset |B|$. The morphisms in* (4) *combined with the natural inclusion $j : \Omega^1_X \otimes \mathcal{M}_{X,D} \to \Omega^1_X(\log B) \otimes \mathcal{M}_{X,D}$ induce the commutative diagram*

$$\begin{array}{ccccc} \mathcal{M}^*_{X,D} & \xrightarrow{i^*} & \mathcal{M}^*_D & \to & 0 \\ \downarrow j \circ d\log & & \downarrow d_D\log & & \\ \Omega^1_X(\log B) \otimes \mathcal{M}_{X,D} & \xrightarrow{i^*} & \Omega^1_X(\log B) \otimes \mathcal{M}_D & \to & 0, \end{array}$$

and its regular version

$$\begin{array}{ccccc} \mathcal{O}^*_X & \xrightarrow{i^*} & \mathcal{O}^*_D & \to & 0 \\ \downarrow & & \downarrow & & \\ \Omega^1_X(\log B) & \xrightarrow{i^*} & \Omega^1_X(\log B) \otimes \mathcal{O}_D & \to & 0. \end{array}$$

Proof. Let $\alpha \in \mathcal{M}^*_D$ and $u \in \mathcal{M}^*_{X,D}$ so that $\alpha = i^*(u)$. By (4), the morphism

$$d_D\log : \mathcal{M}^*_D \to \Omega^1_X(\log B) \otimes \mathcal{M}_D, \quad d_D\log(\alpha) := i^*(j \circ d\log(u))$$

will be well-defined if we show that

$$u \in 1 + I_D\mathcal{M}_{X,D} \Rightarrow d_D\log(u) = 0.$$

So let $u = 1 + h$, for $h \in I_D\mathcal{M}_{X,D}$ a germ at some smooth point of B. Thus B and D have respective local equation $x = 0$ and $x^k = 0$ for some $k \geq 0$, and $h = mx^k$ where $m \in \mathcal{M}_{X,D}$. So

$$d\log(1+h) = \frac{kmx^{k-1}dx + x^k dm}{1 + x^k m} = \frac{mx^k}{1 + x^k m}\big(k\frac{dx}{x} + \frac{dm}{m}\big)$$

belongs to the subsheaf $\Omega^1_X(\log(B)) \otimes I_D\mathcal{M}_{X,D} \subset \Omega^1_X \otimes \mathcal{M}_{X,D}$. By tensoring (2) with the locally free sheaf $\Omega^1_X(\log(B))$ we deduce that

$$i^*(j \circ d\log(1+h)) = 0 \ \in \Omega^1_X(\log B) \otimes \mathcal{M}_D.$$

The divisor B being normal crossing, we check easily that the same conclusion holds when h is a germ at some singular point of B. This implies that the map $d_D \log$ is well-defined, giving the first diagram. The regular version follows by letting $m \in \mathcal{O}_X$ in the previous reasonning and by using the multiplicative version of (1). □

2.2. **Proof of Theorem 2.** We come now to the proof of Theorem 2. We denote by

$$\mathbb{T} := \operatorname{Spec} \mathbb{C}[t_1^{\pm 1}, t_2^{\pm 1}] \quad \text{and} \quad \mathbb{C}^2 := \operatorname{Spec} \mathbb{C}[t_1, t_2]$$

the complex torus of X and the affine plane endowed with canonical coordinates $t = (t_1, t_2)$. We identify rational forms of $\mathbb{T}$ and $\mathbb{C}^2$ with the rational form they induce on X. We suppose from now that $D = 2\operatorname{div}_\infty(f)$ and that $B = X \setminus \mathbb{T}$. The toric surface X being smooth, the toric divisor B is normal crossing. Since f has no poles in the torus, we have $|D| \subset |B|$.

Let $\gamma \in V(D)$. We need to show that γ is linear combinations of the γ_j's. There is no loss of generality to suppose that $\gamma \in V_{\mathbb{Z}}(D)$. Let $\Gamma := C \cap \partial X$ be the intersection of C with the boundary. By hypothesis, we know that

$$\gamma = \sum_{p \in \Gamma} \mu_p \gamma_p \quad \text{and} \quad \gamma = i^*(C_\gamma), \tag{5}$$

where $\gamma_p \in \operatorname{Div}(D)$ is induced by the germ of C at p, μ_p is an integer and where $C_\gamma \in \operatorname{Div}(X)$. Since the torus has a trivial Chow goup, there exists E_γ supported on B so that

$$\operatorname{div}(g) = C_\gamma - E_\gamma$$

for some rational function $g \in \mathbb{C}(X)$. The following key lemma ensures that the poles of the restriction $i^*(dg/g)$ are controled by C.

Lemma 3. *We have $i^*(dg/g) \in H^0(X, \Omega^1_X(\log B) \otimes \mathcal{O}_D(C))$.*

Proof. Obviously, $i^*(dg/g)$ defines a rational section of $\Omega^1_X(\log B) \otimes \mathcal{O}_D$ and we need to show that the germ g_p of g at p satisfies

$$i^*(dg_p/g_p) \in \Omega^1_X(\log B) \otimes \mathcal{O}_D(C)$$

for all $p \in |D|$ (for convenience, we omit the index p in the stalk notations). Let us write $g_p = G_p/H_p$ for some local equations G_p and H_p of respectively C_γ and E_γ. Thus

$$dg_p/g_p = dG_p/G_p - dH_p/H_p. \tag{6}$$

Since E_γ is supported on B, we have $dH_p/H_p \in \Omega^1_X(\log B)$ and it's enough to show that

$$i^*(dG_p/G_p) \in \Omega^1_X(\log B) \otimes \mathcal{O}_D(C)$$

for all $p \in |D|$. For convenience, we let $\gamma_p := 0$ and $\mu_p := 0$ for $p \in |D| \setminus |\Gamma|$. By (5), the germ (C_γ, p) of C_γ at p satisfies

$$i^*(C_\gamma, p) = \mu_p \gamma_p = \mu_p i^*(C, p)$$

for all $p \in |D|$. This is equivalent to that

$$i^*(G_p/F_p^{\mu_p}) \in \mathcal{O}_D^*, \tag{7}$$

where F_p is any local equation of C at p. Lemma 2 combined with (7) implies that

$$d_D \log(i^*(G_p/F_p^{\mu_p})) = i^*(dG_p/G_p) - \mu_p i^*(dF_p/F_p) \in \Omega^1_X(\log B) \otimes \mathcal{O}_D. \tag{8}$$

Since $i^*(dF_p/F_p) \in \Omega^1_X(\log B) \otimes \mathcal{O}_D(C)$, it follows that $i^*(dG_p/G_p)$ belongs to $\Omega^1_X(\log B) \otimes \mathcal{O}_D(C)$. □

Lemma 4. *There exists a unique rational form $\omega \in H^0(X, \Omega^1_X(\log(B) \otimes \mathcal{O}_X(C))$ such that $i^*(dg/g) = i^*(\omega)$.*

Proof. By tensoring (2) with the locally free sheaf $\Omega^1_X(\log B) \otimes \mathcal{O}_X(C)$ and by looking at the associated long exact cohomological sequence, we deduce from Lemma 3 that it is enough to show that

$$H^1(X, \Omega^1_X(\log B) \otimes \mathcal{O}_X(C) \otimes I_D) = 0. \tag{9}$$

But $C - \mathrm{div}_\infty(f) = \mathrm{div}(f)$ being principal, multiplication by f^2 gives a global isomorphism

$$\mathcal{O}_X(C) \otimes I_D \simeq \mathcal{O}_X(-C).$$

Moreover, we know by [13] p. 87 that the sheaf $\Omega^1_X(\log B)$ is globally trivial. Thus, there is a global isomorphism

$$\Omega^1_X(\log B) \otimes \mathcal{O}_X(C) \otimes I_D \simeq \mathcal{O}_X(-C) \oplus \mathcal{O}_X(-C).$$

Since C has a non negative intersection with each irreducible toric divisor of X, the line bundle $\mathcal{O}_X(C)$ is numerically effective ([26], p. 53). Moreover, it is well known ([13], p. 73) that there is equality

$$H^0(X, \mathcal{O}_X(C)) = \{t^m/f,\ m \in N_f \cap \mathbb{Z}^2\}. \tag{10}$$

By (H_1), the Newton polytope N_f has dimension 2, and we deduce from (10) that $\mathcal{O}_X(C)$ is big. It is a standard result that

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

for any big and nef Cartier divisor C on a smooth complete variety X (see [17], Theorem 4.5 for instance). Finally, (9) holds and there exists ω as in Lemma 4. Since $H^0(X, \mathcal{O}_X(-C)) = 0$, the previous reasonning implies that such an ω is unique. □

Up to here, we can show that all previous lemmas would remain valid with the choice $D = \mathrm{div}_\infty(f) + \partial X$ used in [28]. The choice $D \geq 2\,\mathrm{div}_\infty(f)$ appears to be essential in order to have

Lemma 5. *We have $d\omega = 0$.*

Proof. Lemma 1 applied with $F = C$ combined with Lemma 4 gives

$$i^*(d\omega) = d_D(i^*(\omega)) = d_D(i^*(dg/g)) = i^*(d(dg/g)) = 0,$$

where $i^*(d\omega) \in H^0(X, \Omega^2_X(B + 2C) \otimes \mathcal{O}_D)$. By tensoring (2) with $\Omega^2_X(B + 2C)$, and by using the associated long exact cohomological sequence, we deduce that

$$d\omega \in H^0(X, \Omega^2_X(B + 2C) \otimes I_D).$$

Since $2C - D = \mathrm{div}(f^2)$, it follows that $f^2 d\omega \in H^0(X, \Omega^2_X(B))$. By [13] p. 85, the divisor $B = X \setminus \mathbb{T}$ is an anticanonical divisor of X and there is an identification

$$H^0(X, \Omega^2_X(B)) = \mathbb{C}\frac{dt_1 \wedge dt_2}{t_1\, t_2}.$$

Thus,

$$d\omega = \frac{c}{f^2}\frac{dt_1 \wedge dt_2}{t_1\, t_2}$$

for some constant $c \in \mathbb{C}$. This form being exact, its residue at zero vanishes. This forces $c/f^2(0) = res_0(d\omega) = 0$ (recall that $f(0) \neq 0$ by (H_1)) and $d\omega = 0$. □

Here comes a theorem of Ruppert in the picture.

Lemma 6. *There exists some constants $c_j, a_1, a_2 \in \mathbb{C}$ such that*

$$\omega = \sum_{j=1}^{t} c_j \frac{d\bar{q}_j}{\bar{q}_j} + a_1\frac{dt_1}{t_1} + a_2\frac{dt_2}{t_2},$$

with $\bar{q}_1, \cdots, \bar{q}_t$ the irreducible absolute factors of f.

Proof. By [13] p. 87, the map $m \mapsto dt^m/t^m$ gives an isomorphism $\mathbb{Z}^2 \otimes \mathcal{O}_X \simeq \Omega^1_X(\log B)$. We deduce that the map

$$\begin{array}{rcl} H^0(X, \mathcal{O}_X(C)) \oplus H^0(X, \mathcal{O}_X(C)) & \to & H^0(X, \Omega^1_X(\log B) \otimes \mathcal{O}_X(C)) \\ (r_1, r_2) & \mapsto & r_1 dt_1/t_1 + r_2 dt_2/t_2 \end{array}$$

is an isomorphism. It follows from (10) that there exists (unique) polynomials h_1, h_2 such that

$$\omega = \frac{h_1}{f}\frac{dt_1}{t_1} + \frac{h_2}{f}\frac{dt_2}{t_2}, \quad N_{h_i} \subset N_f. \tag{11}$$

On the other hand, ω being closed by Lemma 5, its restriction to $\mathbb{C}^2$ defines an element of the first algebraic De Rham cohomology group $H^1(\mathbb{C}^2 \setminus C_0)$, where

$$C_0 := (C + B) \cap \mathbb{C}^2 = \{t_1 t_2 f = 0\}.$$

By a theorem of Ruppert [23], it follows that there are uniquely determined constants $c_1, \ldots, c_t, a_1, a_2 \in \mathbb{C}$ and a unique *exact* rational 1-form ω' such that

$$\omega - \omega' = \sum_{i=1}^{t} c_j \frac{d\bar{q}_j}{\bar{q}_j} + a_1\frac{dt_1}{t_1} + a_2\frac{dt_2}{t_2}.$$

Since the right hand side can be written as in (11), we deduce that there are polynomials p_1, p_2 so that

$$\omega' = \frac{p_1 dt_1 + p_2 dt_2}{t_1 t_2 f}, \quad \deg(p_i) < \deg(f t_1 t_2),$$

where $\deg(\cdot)$ stands for the total degree. Since the polynomial $t_1 t_2 f$ is reduced (by (H_1) and (H_2)) and ω' is exact, it follows from [6], Proposition 3 that $\omega' = 0$. This gives the desired expression for ω. □

Lemma 7. *Let $\bar{C}_j \in \mathrm{Div}(X)$ be the component of C defined by the absolute factor $\bar{q}_j$. We have the relation $\gamma = \sum_{j=1}^{t} c_j i^*(\bar{C}_j)$.*

Proof. Let $p \in |\Gamma|$ and let $x = 0$ and $y = 0$ be some respective local equations of C and B at p. By Lemma 6, the germ ω_p of ω at p satisfies $\omega_p - c_j\, dy/y \in \Omega^1_X(\log B)$, where $\bar{C}_j$ is the unique component of C passing throw p (unicity of $\bar{C}_j$ comes from (H_2)). It follows that

$$i^*(\omega_p) - c_j i^*(dy/y) \in \Omega^1_X(\log B) \otimes \mathcal{O}_D,$$

while (6) combined with (8) implies that

$$i^*(dg_p/g_p) - \mu_p i^*(dy/y) \in \Omega^1_X(\log B) \otimes \mathcal{O}_D.$$

Using equality $i^*(dg_p/g_p) = i^*(\omega_p)$ induced by Lemma 4, we deduce that

$$(\mu_p - c_j) i^*(dy/y) \in \Omega^1_X(\log B) \otimes \mathcal{O}_D,$$

so that

$$(\mu_p - c_j) i^*(dx \wedge dy/xy) \in \Omega^2_X(B) \otimes \mathcal{O}_D.$$

Hence, there exists $\psi \in \Omega^2_X(B)$ such that

$$(\mu_p - c_j) dx \wedge dy/xy - \psi \in \Omega^2_X(B) \otimes \mathcal{O}_X(C) \otimes I_D.$$

Since $|\operatorname{div}_\infty(f)| = |\partial X|$ (see Subsection 3.1), we deduce that $(D, p) \geq (B, p)$ for any $p \in |\Gamma|$. It follows that the previous germ of 2-form has its polar divisor bounded by the smooth germ of curve $(C, p) = \{y = 0\}$. Hence it has no residue at p

$$\operatorname{res}_p \left[(\mu_p - c_j) dx \wedge dy/xy - \psi \right] = 0.$$

In the same way, $\psi \in \Omega^2_X(B)$ forces $\operatorname{res}_p(\psi) = 0$ so that

$$0 = \operatorname{res}_p \left[(\mu_p - c_j) dx \wedge dy/xy \right] = \mu_p - c_j.$$

The relation $\gamma = \sum_{j=1}^t c_j i^*(\bar{C}_j)$ follows. □

Lemma 8. *γ is $\mathbb{Z}$-combination of the γ_j's.*

Proof. Let $\bar{C}_j$ and $\bar{C}_k$ be conjugate components. We need to show that $c_j = c_k$. Let us consider the schemes X, D , $\bar{C}_j$ and γ as schemes over $\operatorname{Spec} \bar{\mathbb{K}}$ (we keep the same notations for simplicity). Since both D and γ are defined over $\mathbb{K}$, the group $\operatorname{Aut}_{\mathbb{K}}(X)$ of $\mathbb{K}$-automorphisms of X acts on $\operatorname{Div}(D)$ and fix γ. Let $\sigma \in \operatorname{Aut}_{\mathbb{K}}(X)$ be such that $\sigma(\bar{C}_j) = \bar{C}_k$. Then

$$c_k i^*(\bar{C}_k) + \sum_{i \neq k} c_i i^*(\bar{C}_i) = \gamma = \sigma(\gamma) = c_j i^*(\bar{C}_k) + \sum_{i \neq j} c_i \sigma(i^*(\bar{C}_i)). \tag{12}$$

Since σ induces a permutation of the irreducible absolute components of the rational curve C, (12) implies that $(c_j - c_k) i^*(\bar{C}_k)$ is supported on $\sum_{i \neq k} c_i i^*(\bar{C}_i)$. Since by the hypothesis (H_2), the schemes $i^*(\bar{C}_k)$ and $\sum_{i \neq k} i^*(\bar{C}_i)$ have disjoint support, this forces equality $c_j = c_k$. □

This shows that $V(D) = \langle \gamma_1, \ldots, \gamma_s \rangle$. Since the γ_j's have coordinates in $\{0, 1\}$ and are pairwise orthogonal in the canonical basis $(\gamma_P)_{P \in \mathcal{P}}$ of the ambient space V, they form (under some unique permutation) the reduced echelon basis of $V(D)$. Obviously, this remains true for any choice $D \geq 2 \operatorname{div}_\infty(f)$. Theorem 2 is proved. □

Remark 1. *If we rather consider the $\mathbb{Z}$-module $\bar{V}_{\mathbb{Z}}$ induced by the irreducible decomposition of $\gamma_C = C \cap D$ over the algebraic closure $\bar{\mathbb{K}}$ of $\mathbb{K}$, we can check that Theorem 2 remains valid. Namely, if $D \geq 2\,\mathrm{div}_\infty(f)$, then the submodule $\bar{V}_{\mathbb{Z}}(D) \subset \bar{V}_{\mathbb{Z}}$ of divisors that extend to X is free generated by the restrictions of the irreducible absolute components of C. This might be useful to compute the absolute factorization of f.*

3. A toric factorization algorithm

We come now to the proof of Theorem 1. We introduce notations and review basic facts about toric geometry in Subsection 3.1. We describe the echelon basis computation in Subsection 3.2 and the factors computation in Subsection 3.3. We develop a toric factorization algorithm and prove Theorem 1 in Subsection 3.4. We illustrate our results on the example of the introduction.

3.1. **Notations and preliminaries.** We refer to [10], [13] and [26], part II, chapter 1 for an introduction to toric geometry. As before, X designs the smooth toric surface associated to a regular fan Σ that refines the normal fan Σ_f of N_f.

We denote by $D_0, \dots, D_{r+1}$ the irreducible toric divisors of X and by $\rho_0, \dots, \rho_{r+1}$ the corresponding rays of Σ. 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 the convention $\eta_{r+2} = \eta_0$. We denote by $U_i \simeq \mathbb{C}^2$ the affine toric chart associated to the two-dimensional cone $\rho_i \mathbb{R}^+ \oplus \rho_{i+1}\mathbb{R}^+$. Thus,

$$U_i = \mathrm{Spec}\ \mathbb{C}[x, y]$$

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

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

for all $m \in \mathbb{Z}^2$, with $\langle \cdot, \cdot \rangle$ the standard scalar product. Moreover, the irreducible toric divisors have affine equations

$$D_i \cap U_i = \{x = 0\} \quad \text{and} \quad D_{i+1} \cap U_i = \{y = 0\},$$

and $|D_j| \cap U_i = \emptyset$ for $j \notin \{i, i+1\}$. See [26], Lemme 1.1 p. 60.

Since the fan Σ contains the cone generated by the canonical basis (e_1, e_2) of $\mathbb{R}^2$, we can chose the indexation such that $(\eta_{r+1}, \eta_0) = (e_1, e_2)$, in which case

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

It is well known that the toric divisor D_i appears in the principal divisor $\mathrm{div}(f)$ with multiplicity

$$d_i := -min_{m \in N_f} \langle m, \eta_i \rangle.$$

By (H_1), we have $d_0 = d_{r+1} = 0$, and $d_i > 0$ otherwise, so that

$$\mathrm{div}_\infty(f) = d_1 D_1 + \cdots + d_r D_r$$

for some $d_1, \dots, d_r \geq 1$. In particular, $|\,\mathrm{div}_\infty(f)| = |\partial X|$ as asserted in the proof of Lemma 7.

Since $f = \sum_{m \in N_f \cap \mathbb{Z}^2} c_m t^m$, the rational function

$$f_i(x, y) := \sum_{m \in N_f \cap \mathbb{Z}^2} c_m x^{\langle m, \eta_i \rangle + d_i} y^{\langle m, \eta_{i+1} \rangle + d_{i+1}} \tag{13}$$

is a polynomial which does not vanish at $(0,0)$, and C has local equation

$$C \cap U_i = \{f_i(x,y) = 0\}$$

in the chart U_i ([26], Lemma 1.3, p. 62). We call the univariate polynomial $P_i(y) := f_i(0,y)$ the i^{th}-facet polynomial of f, or exterior facet polynomial of f when $i \neq 0, r+1$. The polynomial P_i has degree

$$l_i := \deg(P_i) = \mathrm{Card}(N_f^{(i)} \cap \mathbb{Z}^2) - 1,$$

the lattice length of the i^{th} exterior face

$$N_f^{(i)} := \{m \in N_f,\ \langle m, \eta_i \rangle = -d_i\}$$

of N_f. If ρ_i belongs to the original normal fan Σ_f of N_f, this face has dimension one. Otherwise, it is a vertex of N_f and $l_i = 0$.

A point $p \in C \cap D_i$ has local coordinates $(0, y_p)$ in U_i, where $y_p \in \bar{\mathbb{K}}$ is a root of P_i. Under the hypothesis (H_2), the curve C intersects transversally the boundary of X so that there exists a unique series $\phi_p \in \bar{\mathbb{K}}[[x]]$ such that $\phi_p(0) = y_p$ and $f_i(x, \phi_p) \equiv 0$. The restriction γ_p of the germ of C at p to an effective toric divisor $D = \sum k_i D_i$ is thus uniquely determined by the truncation at order k_i of the series ϕ_p. Since the ϕ_p's are conjugate when the y_p's run over the roots of an irreducible rational factor P of P_i, the Cartier divisor of D

$$\gamma_P := \sum_{P(y_p)=0} \gamma_p$$

is defined and irreducible over $\mathbb{K}$. It follows that the restriction γ_C of C to D admits the irreducible *rational* decomposition

$$\gamma_C = \sum_{P \in \mathcal{P}} \gamma_P,$$

where $\mathcal{P} := \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_r$ is the union of the sets $\mathcal{P}_i$ of the non constant monic irreducible rational factors of the i^{th} exterior facet polynomial of f.

3.2. **Computing the reduced echelon basis. Proof of Theorem 2.** We now give a way to compute the reduced echelon basis of $V(D) \subset V$ when $D = 2\,\mathrm{div}_\infty(f)$. So we need criterions for lifting Cartier divisors from D to X. In [28], the author obtain such conditions that involves the algebraic coefficients of the series ϕ_p's. From an effective point of view, we rather follow [8] and work over the residue field

$$\mathbb{K}_P := \mathbb{K}[y]/(P(y))$$

associated to each $P \in \mathcal{P}$. Let y_P be the residual class of y. A series $\mathrm{B} \in \mathbb{K}_P[[x]]$ can be uniquely written

$$\mathrm{B} = \sum_{j=0}^{l_p - 1} b_j y_P^j$$

where $l_P := \deg(P)$ and $b_j := \mathrm{coeff}(\mathrm{B}, y_P^j) \in \mathbb{K}[[x]]$. For convenience, we denote by $\mathrm{coeff}_k(\mathrm{B}, y_P^j) \in \mathbb{K}$ the coefficient of x^k in b_j.

Suppose that $P \in \mathcal{P}_i$. Under the hypothesis (H_2), there exists a unique power series $\phi_P \in \mathbb{K}_P[[x]]$ such that $f_i(x, \phi_P) \equiv 0$ and $\phi_P(0) = y_P$. So ϕ_P is the conjugate

class of the series ϕ_p associated to the roots of P. Note that ϕ_P is invertible. For all integer $k \neq 0$, we define

$$\mathrm{B}^k(\phi_P) := \frac{\phi_P^k}{k} \in \mathbb{K}_P[[x]],$$

and we define $\mathrm{B}^0(\phi_P) := \log(\phi_P)$ to be the unique primitive of ϕ_P'/ϕ_P which vanishes at 0 . For all $m \in \mathbb{Z}^2$, we define

$$a_{Pm} := \sum_{j=0}^{l_P-1} \mathrm{Tr}^j(P)\, \mathrm{coeff}_{-\langle m,\eta_i\rangle}(\mathrm{B}^{\langle m,\eta_{i+1}\rangle}(\phi_P), y_P^j),$$

where i is chosen so that $P \in \mathcal{P}_i$ and where $\mathrm{Tr}^j(P)$ designs the sum of the j^{th} power of the roots of P. So $a_{Pm} \in \mathbb{K}$. Theorem 3 follows from the following

Proposition 1. *Let M denote the set of interior lattice points of $2N_f$ and let A denote the matrix $(a_{Pm})_{P\in\mathcal{P},\, m\in M}$. There is equality $V(D) = \ker(A)$.*

Proof. By the algebraic osculation Theorem 1 in [28], we know that there exists a pairing

$$\langle\cdot,\cdot\rangle_D : \mathrm{Div}(D) \otimes \mathbb{C} \times H^0(X, \Omega_X^2(D)) \to \mathbb{C}$$

such that $\gamma \in \mathrm{Div}(D)$ extends to X if and only if $\langle\gamma,\cdot\rangle_D \equiv 0$. Since $D = 2\,\mathrm{div}_\infty(f)$, we have

$$H^0(X, \Omega_X^2(D)) = \bigoplus_{m\in M} \mathbb{C}\,\psi_m, \quad \psi_m := t^m \frac{dt_1 \wedge dt_2}{t_1 t_2}$$

and the explicit formula in [28] (Proposition 1) gives equality

$$\langle\gamma_p, \psi_m\rangle_D = \mathrm{coeff}(\mathrm{B}^{\langle m,\eta_{i+1}\rangle}(\phi_p), x^{-\langle m,\eta_i\rangle})$$

for all $p \in C \cap D_i$. Note that $-\langle m, \eta_i\rangle < 2d_i$ by hypothesis, so that the previous expression only depends on ϕ_p modulo (x^{2d_i}).

Suppose that y_p is a root of $P \in \mathcal{P}_i$. Since ϕ_P is the conjugate class of ϕ_p, there exists for all $k \in \mathbb{Z}$ a unique polynomial $\mathrm{R}^k \in \mathbb{K}[x][y]$ with degree $< 2d_i$ in x and degree $< l_P$ in y such that

$$\mathrm{B}^k(\phi_P) \equiv \mathrm{R}^k(y_P) \bmod (x^{2d_i}) \quad \text{and} \quad \mathrm{B}^k(\phi_p) \equiv \mathrm{R}^k(y_p) \bmod (x^{2d_i}).$$

Hence, we have congruence relations

$$\sum_{P(y_p)=0} \mathrm{B}^k(\phi_p) \equiv \sum_{P(y_p)=0} \sum_{j=0}^{l_P-1} \mathrm{coeff}(\mathrm{R}^k, y^j) y_p^j \equiv \sum_{j=0}^{l_P-1} \mathrm{Tr}^j(P)\, \mathrm{coeff}(\mathrm{B}^k(\phi_P), y_P^j)$$

modulo (x^{2d_i}) and the relation

$$\langle\gamma_P, \psi_m\rangle_D = \sum_{P(y_p)=0} \langle\gamma_p, \psi_m\rangle_D = a_{Pm}$$

follows. So $\gamma \in V_{\mathbb{Z}}$ extends to a Cartier divisor on X if and only if $\gamma A = 0$. It follows that $V(D) = \ker(A)$. □

Let us look at the algorithmic complexity underlying Proposition 1. Following [15], we use notation $\widetilde{\mathcal{O}}$ for soft $\mathcal{O}$, and we let $2 < \omega < 2.34$ be the matrix multiplication exponent. We recall that the complexity for multiplying two polynomials of degree d belongs to $\widetilde{\mathcal{O}}(d)$ (Schönhage and Strassen algorithm, [15]).

Corollary 1. *Suppose given the rational factorization of the exterior facet polynomials of f. We can build the matrix A with $\widetilde{\mathcal{O}}(\mathrm{Vol}(N_f)^2)$ arithmetic operations in $\mathbb{K}$ and then compute the reduced echelon basis of $V(D)$ with $\mathcal{O}(\mathrm{Vol}(N_f)\,\mathrm{Card}(\mathcal{P})^{\omega-1})$ arithmetic operations in $\mathbb{K}$.*

Proof. We divide the proof in three steps.

Step 1. Computing the ϕ_P's. We use the classical Newton iteration algorithm [15]. In order to estimate the cost in our toric setting, we need the following

Lemma 9. *Let $P \in \mathcal{P}_i$, $\phi \in \mathbb{K}_P[[x]]$ and let $f_i \in \mathbb{K}[x,y]$ as defined in* (13)*. For any $k \in \mathbb{N}$, we can evaluate $f_i(x,\phi) \in \mathbb{K}_P[[x]]$ modulo (x^k) with $\widetilde{\mathcal{O}}(k\,\mathrm{Vol}(N_f))$ arithmetic operations in $\mathbb{K}_P$.*

Proof. Since f_i is a sum of $\mathcal{O}(\mathrm{Vol}(N_f))$ monomials, we can evaluate $f_i(x,\cdot)$ at ϕ modulo (x^k) by evaluating each of the involved monomials with $\mathcal{O}(\mathrm{Vol}(N_f)\log(n_i))$ operations in $\mathbb{K}_P[[x]]/(x^k)$, where n_i is the total degree of f_i in y. All what we need to show is that n_i is not "too big". By (13), we have

$$n_i := \deg_y(f_i) = \max_{m\in N_f} \langle m, \eta_{i+1}\rangle - \min_{m\in N_f} \langle m, \eta_{i+1}\rangle,$$

Let $m \in N_f$. By (H_1), the polytope $\mathrm{Conv}\{(0,0),(1,0),(0,1),m\}$ is contained in N_f. Since it has euclidean volume $(m_1+m_2)/2$, we deduce $\|m\| \in \mathcal{O}(\mathrm{Vol}(N_f))$ for all $m \in N_f$, where $\|m\| := |m_1| + |m_2|$. There remains to estimate $\|\eta_{i+1}\|$. As before, we check easily that $\|\eta\| \in \mathcal{O}(\mathrm{Vol}(N_f))$ for all inward primitive normal vectors of the *one dimensional* faces of N_f. Let $j > i$ be the first index for which the j^{th}-exterior face of N_f has dimension one. So we can write $\eta_{i+1} = a\eta_i + b\eta_j$ for some positive rational numbers a, b. We have relations

$$b\det(\eta_i,\eta_j) = \det(\eta_i,\eta_{i+1}) = 1 \quad \text{and} \quad a\det(\eta_i,\eta_j) = \det(\eta_{i+1},\eta_j) < \det(\eta_i,\eta_j),$$

last inequality using that Σ is regular and refines Σ_f (see [9]). So $a, b \leq 1$. Since $\|\eta_i\| \in \mathcal{O}(\mathrm{Vol}(N_f))$ and $\|\eta_j\| \in \mathcal{O}(\mathrm{Vol}(N_f))$, it follows that $\|\eta_{i+1}\| \in \mathcal{O}(\mathrm{Vol}(N_f))$. Since $|\langle m, \eta_{i+1}\rangle| \in \mathcal{O}(\|m\|\|\eta_{i+1}\|)$, we deduce $n_i \in \mathcal{O}(\mathrm{Vol}(N_f)^2)$.

Hence, the cost for the evaluation step is $\mathcal{O}(\mathrm{Vol}(N_f)\log(\mathrm{Vol}(N_f)))$ operations in $\mathbb{K}_P[[x]]/(x^k)$, or $\widetilde{\mathcal{O}}(k\,\mathrm{Vol}(N_f))$ operations in $\mathbb{K}_P$ (Corollary 9.7, [15]). □

By using the fast modular Newton iteration Algorithm 2, [8] and by replacing the given evaluation cost by that induced by Lemma 9, we deduce that we can compute the series ϕ_P with precision $2d_i$ with $\widetilde{\mathcal{O}}(d_i\,\mathrm{Vol}(N_f))$ operations in $\mathbb{K}_P$. Each operation in $\mathbb{K}_P$ takes $\widetilde{\mathcal{O}}(l_P)$ operations in $\mathbb{K}$ and we have $\sum_{P\in\mathcal{P}_i} l_P = l_i$. Since $2C$ and D have the same Picard class, we deduce

$$\sum_{i=1}^{r} 2d_i l_i = \sum_{i=1}^{r} 2d_i \deg(C\cdot D_i) = \deg(C\cdot D) = 2\deg(C\cdot C) = 4\,\mathrm{Vol}(N_f),$$

the last equality using basic toric intersection theory (see [13] for instance). It follows that computing all the ϕ_P's up to the precision imposed by D has complexity $\widetilde{\mathcal{O}}(\mathrm{Vol}(N_f)^2)$.

Step 2. Building the matrix A. Let $P \in \mathcal{P}_i$. Computing the series $\mathrm{B}^{\langle m,\eta_{i+1}\rangle}(\phi_P)$ with precision $2d_i$ for all $m \in \mathrm{int}(2N_f) \cap \mathbb{Z}^2$ requires at most one inversion in $\mathbb{K}_P[[x]]/(x^{2d_i})$ and $\mathcal{O}(\mathrm{Vol}(N_f))$ evaluations of monomials in $\mathbb{K}_P[[x]]/(x^{2d_i})[y]$ of degrees bounded by $n_i = \mathcal{O}(\mathrm{Vol}(f)^2)$ (and possibly the computation of a primitive of ϕ'_P/ϕ_P modulo (x^{2d_i})). Each operation takes $\widetilde{\mathcal{O}}(l_P d_i)$ operations in $\mathbb{K}$, giving a total number of $\widetilde{\mathcal{O}}(\mathrm{Vol}(N_f) l_P d_i)$ operations in $\mathbb{K}$. Summing up over all $P \in \mathcal{P}$, we obtain a total number of $\widetilde{\mathcal{O}}(\mathrm{Vol}(N_f)^2))$ operations in $\mathbb{K}$ for computing all the $\mathrm{B}^k(\phi_P)$ involved in the definition of A. Then building the matrix A has a negligeable cost.

Step 3. Computing the reduced echelon basis of $V(D)$. Since $V(D)$ is determined by $\mathcal{O}(\mathrm{Vol}(N_f))$ equations and $\mathrm{Card}(\mathcal{P})$ unknowns, we can compute its reduced echelon basis with $\mathcal{O}(\mathrm{Vol}(N_f)\,\mathrm{Card}(\mathcal{P})^{\omega-1})$ operations in $\mathbb{K}$ ([24], Theorem 2.10). □

3.3. **Factors computation.** We want now to compute the rational factors of f. In all of this section, we fix γ in the reduced echelon basis of $V(D)$ and we denote by q the corresponding factor f. We first compute the Newton polytope of q. By a Theorem of Ostrovski [22], N_q is a Minkovski summand of N_f so that it is enough to compute the integers

$$e_i := -min_{m\in N_q}\langle m, \eta_i\rangle, \quad i = 0, \dots, r+1.$$

Suppose that $\gamma = \sum_{P\in\mathcal{P}} \mu_P \gamma_P$. We define

$$l_i(\gamma) := \sum_{P\in\mathcal{P}_i} \mu_P \deg(P)$$

for all $i = 1, \dots, r$. We obtain the following

Proposition 2. *We have $e_0 = e_{r+1} = 0$ and the integers $e_1, \dots, e_r$ are the unique solutions of the affine system*

$$\sum_{i=1}^{r} e_i a_{ij} = l_j(\gamma), \quad j = 1, \dots, r,$$

with $a_{i,i+1} := 1$, $a_{ii} := \det(\eta_{i-1}, \eta_{i+1})$ and $a_{ij} := 0$ for $j \neq i, i+1$.

Proof. Since N_q is a Minkowski summand of N_f, the hypothesis (H_1) forces $0 \in N_q$, so that $e_0 = e_{r+1} = 0$, and $e_i \geq 0$ otherwise. By Subsection 3.1, we know that

$$\mathrm{div}_\infty(q) = e_1 D_1 + \cdots + e_r D_r$$

while the component $C' = \mathrm{div}_0(q)$ of C satisfies

$$\deg(C' \cdot D_j) = \deg(\gamma_{|D_j}) = l_j(\gamma), \quad j = 1, \dots, r. \tag{14}$$

Now, the Chow group of the smooth affine plane completion X is $\mathbb{Z}$-free generated by the classes of $D_1, \dots, D_r$ and numerical and rational equivalence coincide on a

smooth toric variety [26], p.53. By duality, it follows that (14) uniquely determines the class of C', that is the class of $\mathrm{div}_\infty(q)$, that is the integers $e_1, \dots, e_r$. We have equality

$$\deg(C' \cdot D_j) = \deg(\mathrm{div}_\infty(q) \cdot D_j) = \sum_{i=1}^{r} e_i \deg(D_i \cdot D_j)$$

and it's well known that $\deg(D_i \cdot D_j) = a_{ij}$ ([13], chapter 5.1, p. 99). Proposition 2 follows. Note that $\det(a_{ij}) = \pm 1$. □

We can now consider $q(t) = \sum_{m \in N_q \cap \mathbb{Z}^2} c_m t^m$ as a vector indexed by the lattice points of N_q. For all $m \in N_q$ and all $P \in \mathcal{P}$, we define

$$r_{Pm} \in \mathbb{K}_P[[x]]/(x^{e_i+1}), \qquad r_{Pm} := x^{\langle m, \eta_i \rangle + e_i} \phi_P^{\langle m, \eta_{i+1} \rangle} \bmod (x^{e_i+1}),$$

where i is chosen so that $P \in \mathcal{P}_i$. This definition makes sense since ϕ_P is invertible and $\langle m, \eta_i \rangle + e_i \geq 0$ for all $m \in N_q$. We obtain the following

Proposition 3. *Under normalization $q(0) = 1$, the coefficients vector $(c_m)_{m \in N_q \cap \mathbb{Z}^2}$ of q is the unique rational solution of*

$$c_0 = 1 \quad \textit{and} \quad \sum_{m \in N_q \cap \mathbb{Z}^2} c_m r_{Pm} = 0 \in \mathbb{K}_P[[x]]/(x^{e_i+1}) \quad \forall P \in \mathcal{P},\ \mu_P \neq 0.$$

The induced system (S_γ) over $\mathbb{K}$ contains $\mathcal{O}(\mathrm{Vol}(N_q))$ affine equations.

Proof. Let $h \in \mathbb{K}[t_1, t_2]$ with Newton polytope contained in N_q. So h and q define global sections of the line bundle $\mathcal{O}_X(E)$, where $E := \sum_{i=1}^r e_i D_i$. In particular $h = \lambda q$ for $\lambda \in \mathbb{C}$ if and only if the two Cartier divisors $H := \mathrm{div}(h) - E$ and $C' := \mathrm{div}(q) - E$ are equal. Since the restriction

$$H^0(X, \mathcal{O}_X(E)) \to H^0(X, \mathcal{O}_{E+\partial X}(E))$$

is injective and H and C' are rationally equivalent to E, we deduce that

$$\begin{aligned} C' = H \quad &\iff \quad C' \cap (E + \partial X) = H \cap (E + \partial X) \\ &\iff \quad C' \cap (E + \partial X) \subset H, \end{aligned}$$

with intersection and inclusion taken scheme theoretically. Since $N_q \subset N_f$, we have $E \leq \mathrm{div}_\infty(f)$, so that $E + \partial X \leq D$ and

$$C' \cap (E + \partial X) = \gamma \cap (E + \partial X) = \bigcup_{\mu_P \neq 0} \gamma_P \cap (E + \partial X).$$

Let $h_i = 0$ be the local equation of H in the chart U_i. For $P \in \mathcal{P}_i$, we know that $\gamma_P \cap (E + \partial X) = \gamma_P \cap (e_i + 1) D_i$ is contained in U_i. Hence, we have equivalence

$$\gamma_P \cap (e_i + 1) D_i \subset H \iff h_i(x, \phi_P(x)) \equiv 0 \mod (x^{e_i+1}).$$

If $h(t) = \sum_{m \in N_q \cap \mathbb{Z}^2} u_m t^m$, we can suppose that (following (13))

$$h_i(x, y) := \sum_{m \in N_q \cap \mathbb{Z}^2} u_m x^{\langle m, \eta_i \rangle + e_i} y^{\langle m, \eta_{i+1} \rangle + e_{i+1}}.$$

Since ϕ_P is invertible, we obtain by linearity that $\gamma_P \cap (E + \partial X) \subset H$ is equivalent to that equality $\sum_m u_m r_{Pm} = 0$ holds in $\mathbb{K}_P[[x]]/(x^{e_i+1})$. It follows that q is the unique solution of the announced system of equations.

A linear equation in $\mathbb{K}_P[[x]]/(x^{e_i+1})$ being equivalent to a system of $l_P(e_i+1)$ equations over $\mathbb{K}$, the total number of equations of the induced system (S_γ) over $\mathbb{K}$ is

$$\begin{aligned} 1 + \sum_{i=1}^{r} \sum_{P \in \mathcal{P}_i} (e_i+1)\mu_P l_P &= 1 + \sum_{i=1}^{r} (e_i+1)\deg(C' \cdot D_i) \\ &= \deg(C' \cdot E) + \deg(C' \cdot \partial X) + 1 \in \mathcal{O}(\mathrm{Vol}(N_q)). \end{aligned}$$

□

We deduce the following

Corollary 2. *Suppose given the reduced echelon basis of $V(D)$. We can compute all the irreducible rational factors of f with at most $\mathcal{O}(\mathrm{Vol}(N_f)^\omega)$ arithmetic operations in $\mathbb{K}$.*

Proof. Let γ belongs to the reduced echelon basis of $V(D)$. Once the affine system (S_γ) is built, Proposition 3 allows us to compute the corresponding factor q of f by solving a system of $\mathcal{O}(\mathrm{Vol}(N_q))$ affine equations over $\mathbb{K}$ and $\mathcal{O}(\mathrm{Vol}(N_q))$ unknowns. This requires $\mathcal{O}(\mathrm{Vol}(N_q)^\omega)$ arithmetic operations in $\mathbb{K}$ (Theorem 2.10 in [24]). There remains to build the system. Computing N_q using Proposition 2 has a negligeable cost. Let $P \in \mathcal{P}_i$. We need to compute ϕ_P with precision x^{e_i+1}. Since $e_i \leq d_i$ and $d_i > 0$, we have $e_i + 1 \leq 2d_i$ so that ϕ_P has already been computed with a sufficient precision. In the same way, computing the involved powers $\phi_P^{\langle m, \eta_{i+1} \rangle}$, $m \in N_q$ from the already computed powers $\phi_P^{\langle m, \eta_{i+1} \rangle}$, $m \in \mathrm{int}(2N_f \cap \mathbb{Z}^2)$ has a negligeable cost too. If $f = q_1 \cdots q_s$ is the rational factorization of f, we have inequality

$$\mathrm{Vol}(N_{q_1}) + \cdots + \mathrm{Vol}(N_{q_s}) \leq \mathrm{Vol}(N_{q_1} + \cdots + N_{q_s}) = \mathrm{Vol}(N_f)$$

and we finally need at most

$$\mathcal{O}(\mathrm{Vol}(N_{q_1})^\omega + \cdots + \mathrm{Vol}(N_{q_s})^\omega) \subset \mathcal{O}(\mathrm{Vol}(N_f)^\omega)$$

arithmetic operations in $\mathbb{K}$ for computing the rational factorization of f from the reduced echelon basis. □

Let us remark that the system (S_γ) has a particular sparse structure. For instance, it contains the subsystems of type Vandermond

$$\sum_{m \in N_q^{(i)} \cap \mathbb{Z}^2} c_m y_P^{\langle m, \eta_{i+1} \rangle} = 0, \quad P \in \mathcal{P}_i,\ \mu_P \neq 0$$

that determines (up to multiplication by some constant) the i^{th} exterior facet polynomial $\prod_{P \in \mathcal{P}_i} P^{\mu_P}$ of q. We might hope that in practice, the resolution of S_γ is relatively fast.

3.4. **A toric factorization algorithm. Proof of Theorem 1.** By combining all previous results, we deduce the following

Toric Factorization Algorithm (TFA).

Input: $f \in \mathbb{K}[t_1, t_2]$ satisfying hypothesis (H_1) and (H_2).

Output: The irreducible factorization $f = q_1 \cdots q_s$ of f over $\mathbb{K}$.

Step 0. Compute a regular fan Σ which refines Σ_f.

Step 1. Compute the set $\mathcal{P}$ of the irreducible rational factors of the exterior facet polynomials of f.

Step 2. For $i = 1, \ldots, r$ and $P \in \mathcal{P}_i$, compute the series $\phi_P \in \mathbb{K}[[x_i]]$ with precision $x_i^{2d_i}$ using modular Newton iteration.

Step 3. Compute the suitable powers of the ϕ_P's in order to build the matrix A of Proposition 1.

Step 4. Compute the reduced echelon basis of $V(D)$.

Step 5. Compute the rational factors of f by using Propositions 2 and 3.

Theorem 1 follows immediately from the following

Proposition 4. *The algorithm TFA is correct. It requires to factorize the exterior facet polynomials and to perform at most* $\mathcal{O}(\mathrm{Vol}(N_f)^\omega)$ *arithmetic operations in* $\mathbb{K}$.

Proof. The correctness of the algorithm is a consequence of Theorem 2 and Propositions 1, 2, 3. The desingularization of the fan Σ can be obtained by computing some Hirzebruch continued fractions (see [9]) and has a negligeable cost. We consider rational univariate factorization as a black-box of our algorithm. See for instance [15], [21] and [4] for recent advances in that direction. Finally, the cost of steps $2, 3, 4, 5$ follows from Corollaries 1 and 2. □

3.5. **A detailed example.** The bold representation used in that example permits to identify the various objects associated to one of the exterior facets.

Suppose that we want to factorize $f(t) = \mathbf{-16t_1^4t_2^4 - 10t_1^3t_2^2 - t_1^2} + 38t_1^3t_2^3 + 2t_1^2t_2^4 + 16t_1^2t_2^3 - 2t_2^3 + 10t_1^2t_2^2 - 4t_1t_2^3 + 7t_1^2t_2 - 5t_1t_2^2 - 3t_1t_2 - 3t_2^2 + 2t_1 + 2t_2 + 3$ over the field of rational numbers $\mathbb{K} = \mathbb{Q}$.

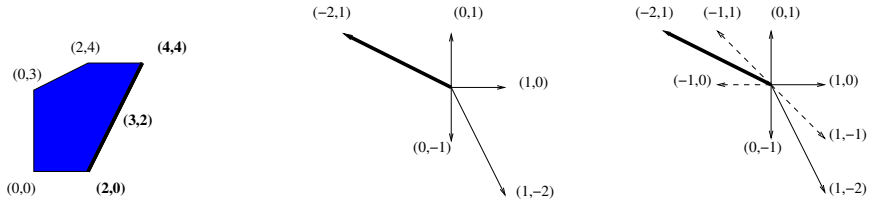

FIGURE 2. The Newton polytope N_f, its normal fan Σ_f and a refined regular fan Σ with the added rays in dots.

We first compute the refined fan Σ (step 0). We obtain here $r = 6$ and

$(\eta_1, d_1, l_1) = ((-1,1),2,0)$, $(\eta_{\mathbf{2}}, \mathbf{d_2}, \mathbf{l_2}) = ((\mathbf{-2},\mathbf{1}),\mathbf{4},\mathbf{1})$, $(\eta_3, d_3, l_3) = ((-1,0),4,0)$,

$(\eta_4, d_4, L_4) = ((0,-1),4,2)$, $(\eta_5, d_5, l_5) = ((1,-2),6,2)$, $(\eta_6, d_6, l_6) = ((1,-1),3,0)$.

There are 3 non constant exterior facets polynomials $\mathbf{P_2} = \mathbf{y^2 + 10y + 16}$, $P_4 = y^2 - 1/8$ and $P_5 = y - 1$. We have $P_2 = (y+2)(y+8) =: P_{21}P_{22}$ while P_4 and P_5 are irreducible over $\mathbb{Q}$. So $\mathcal{P} = \{\mathbf{P_{21}}, \mathbf{P_{22}}, P_4, P_5\}$ (step 1). We lift each facet factor to a local analytic factor with respective precisions $\mathbf{2d_2} = \mathbf{8}, \mathbf{2d_2} = \mathbf{8}$, $2d_4 = 8$ and $2d5 = 12$ (step 2). We obtain in such a way the local decomposition $\gamma_C = \gamma_{\mathbf{P_{21}}} + \gamma_{\mathbf{P_{22}}} + \gamma_{P_4} + \gamma_{P_5}$ of the restriction of C to $D = 2\,\mathrm{div}_\infty(f)$.

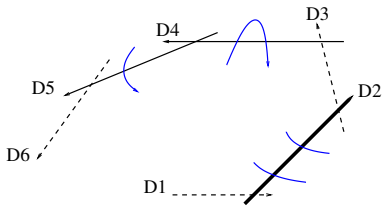

FIGURE 3. The local decomposition of the curve C of f in a neighborhood of the boundary of the smooth toric surface X. The curve does not intersect the exceptional divisors (in dots) corresponding to the added rays of Σ.

We have $\mathrm{Card}(\mathcal{P}) = 4$ and the number of interior lattice points of $2N_f$ is 32. We build the recombination matrix A (4 lines and 32 columns) by using Proposition 1 (step 3). We obtain

$$A = \begin{pmatrix} -2 & 1/2 & 0 & 0 & 0 & 0 & -7/2 & 1 & -1/8 & \dots \\ -3/8 & 1/8 & 0 & 0 & 0 & 0 & 7/128 & 3/64 & -1/128 & \dots \\ 3/8 & -1/8 & 0 & 0 & 0 & 0 & -7/128 & -3/64 & 1/128 & \dots \\ 2 & -1/2 & 0 & 0 & 0 & 0 & 7/2 & -1 & 1/8 & \dots \end{pmatrix}$$

We compute the reduced echelon basis of $\ker(A)$ (step 4). We obtain $\mathcal{B} = (\gamma_1, \gamma_2) = \big((1,0,0,1),(0,1,1,0)\big)$. We deduce the irreducible decomposition $C = C_1 \cup C_2$, where

$$C_1 \cap D = \gamma_1 = \gamma_{P_{21}} + \gamma_{P_5} \quad \text{and} \quad C_2 \cap D = \gamma_2 = \gamma_{P_{22}} + \gamma_{P_4}.$$

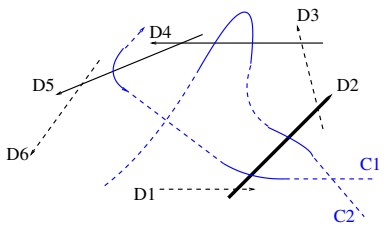

FIGURE 4. The recombination problem is solved.

The intersection numbers $l_1(\gamma_1) = 0$, $\mathbf{l_2}(\gamma_\mathbf{1}) = \mathbf{1}$, $l_3(\gamma_1) = 0$, $l_4(\gamma_1) = 0$, $l_5(\gamma_1) = 1$, $l_6(\gamma_1) = 0$ of the curve C_1 with the components $D_1, \ldots, D_6$ of the boundary (respectively $l_1(\gamma_2) = 0$, $\mathbf{l_2}(\gamma_\mathbf{2}) = \mathbf{1}$, $l_3(\gamma_2) = 0$, $l_4(\gamma_2) = 2$, $l_5(\gamma_2) = 0$, $l_6(\gamma_2) = 0$ for the curve C_2) correspond to the lattice length of the exterior facets of the Newton polytopes of the corresponding factors q_1 and q_2 of f. We deduce the corresponding Minkowski decomposition of N_f thanks to Proposition 2.

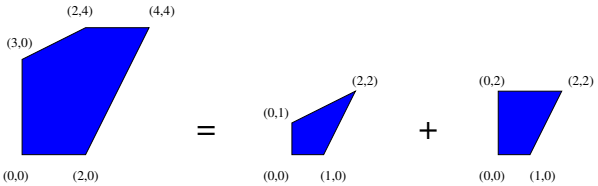

FIGURE 5. The Newton polytopes of the factors q_1 and q_2 of f. We have equality $N_f = N_{q_1} + N_{q_2}$ by a theorem of Ostrowski [22].

Now that we know both the polytopes of the factors and the Taylor expansion of their curves at the toric infinity with a suitable precision, the factors computation (step 5) is reduced to linear algebra thanks to Proposition 3. We finally obtain the irreducible rational factorization

$$f(t) = \big(3 + 2t_2 + 4t_1t_2 - \mathbf{t_1} - \mathbf{2t_1^2t_2^2}\big)\big(1 - t_2^2 - 3t_1t_2 + \mathbf{t_1} + \mathbf{8t_1^2t_2^2}\big).$$

Let us remark that using the smaller lifting precision $D = \mathrm{div}_\infty(f)$ (corresponding to the first 7 columns of the matrix A) would have been here sufficient in order to solve the recombination problem and to compute the factorization of f.

4. Comparison with related results. Improvements

In Subsection 4.1, we compare the algorithm TFA with the most related dense algorithms. In Subsection 4.2, we discuss the relation with the toric algorithm developed in [28] by the author. In particular, we obtain a sufficient criterion for using a smaller lifting precision.

4.1. **Comparison with dense algorithms.**

We compare our method with the lifting and recombination scheme proposed by Lecerf [18], [19] and Chèze-Lecerf [8] for dense polynomials and we discuss some possible improvements for each step of the algorithm TFA.

About Step 0. Since $C \cap D_i = 0$ for all rays $\rho_i \in \Sigma \setminus \Sigma_f$, we need not to compute all the fan Σ. Namely, we check easily that it's enough to compute the succesive rays $\rho_{i+1} \in \Sigma$ of the rays $\rho_i \in \Sigma_f$.

About Step 1. In most cases, the cost of the univariate factorization step dominates the complexity of the algorithm TFA. It might be interesting to avoid some of the facet factorization by chosing D with support strictly contained in $|\partial X|$. For instance, if f has bidegree (d_1, d_2), then $X = \mathbb{P}^1 \times \mathbb{P}^1$ and we might hope to recover the decomposition of C from its restriction to $D = (d_1 + 1)\mathbb{P}^1$ since the corresponding restriction $H^0(X, \mathcal{O}_X(C)) \to H^0(X, \mathcal{O}_D(C))$ is injective. This turns out to be the case : in [18], G. Lecerf factorizes bidegree polynomials by using only one facet factorization with a sharp precision. In general, D has to obey to

the vanishing cohomological properties used in the proof of Theorem 2, which are closely connected with the geometry of N_f.

About Step 2. In the dense absolute case treated in [8], G. Lecerf and G. Chèze compute the analoguous series by introducing the Paterson-Stockmeyer evaluation scheme in the Newton iteration process. We can adapt such a method to our situation by replacing the input polynomial of Algorithm 1, [8] by a polynomial with degree bounded by $\mathrm{Vol}(N_f)$. In such a way, the complexity $\mathcal{O}(\mathrm{Vol}(N_f)^2)$ of step 2 decreases to $\widetilde{\mathcal{O}}(\mathrm{Vol}(N_f)^{(\omega+1)/2})$.

About Step 3. In [18], G. Lecerf builds an analoguous linear system by using fast modular euclidean divison rather than by computing the ϕ_P's powers. Both approaches give rise to equivalent linear systems (see [5], Section 2.3), but the divison method permits to build the underlying matrix faster. We might hope that in the toric case, it is possible too to introduce an equivalent matrix that can be built using modular division.

About Step 4. In [18] and [19], the linear system resolution has complexity $\mathcal{O}(d^{\omega+1})$ with d the total degree of f. It's easy to check that the sum of the lattice lengths of the exterior facets of N_f is bounded by d, with equality if and only if Σ_f is regular. It follows that $\mathrm{Card}(\mathcal{P}) \leq d$. Since $\mathcal{O}(\mathrm{Vol}(N_f)) \subset \mathcal{O}(d^2)$, the reduced echelon basis computation is faster using the toric approach (much faster in the most case).

About Step 5. Since we recover the factors of f by solving affine systems, step 5 has a relatively high cost in the algorithm TFA. If f is a dense polynomial, the task is much simpler and we can recover fastly the global factors of f from the local ones by using modular multiplications of (see [18]), or by using a partial fraction decomposition method (see [8], [1]). This permits a softly d^3 complexity for the factors computation, in general much faster than our approach. We might hope to adapt these methods to the toric case.

4.2. **About the lifting precision.** In [19], G. Lecerf gives an example in the dense case that shows that the precision $D := 2\,\mathrm{div}_\infty(f)$ is sharp in Theorem 2. On an other hand, the author obtain in [28] a toric factorization algorithm running with precision $E := \mathrm{div}_\infty(f) + \partial X$, but with exponential complexity in most cases. We explain here the relation with our algorithm and we give an explicit sufficient criterion for using the precision $E < D$.

Let $\gamma = \sum_{P\in\mathcal{P}} \mu_P \gamma_P \in V$. We define the rational numbers

$$l_i(\gamma) := \sum_{P\in\mathcal{P}} \mu_P \deg(P), \quad i = 1, \ldots, r$$

and we introduce the following convex subset of V

$$\Delta_C = \Big\{\gamma \in V, \quad \sum_{i=1}^{r} \langle e_k, \eta_i\rangle l_i \leq \sum_{i=1}^{r} \langle e_k, \eta_i\rangle l_i(\gamma) \leq 0, \quad k = 1, 2\Big\},$$

where (e_1, e_2) is the canonical basis. We have the following

Proposition 5. *The finite set $V(E) \cap \{0,1\}^{\mathcal{P}} \cap \Delta_C$ is a system of generators of the vector subspace $V(D) \subset V(E)$.*

Proof. Since $V(D)$ admits a basis with coordinates in $\{0,1\}$, it's enough to show that $V(D)\cap\{0,1\}^{\mathcal{P}} = V(E)\cap\{0,1\}^{|\Gamma|}\cap\Delta_C$. Let $\gamma\in V(D)\cap\{0,1\}^{\mathcal{P}}$. So γ is restriction to D of a rational component $C'\in\mathrm{Div}(X)$ of C (Theorem 2). In particular, both divisors C' and $C-C'$ are numerically effective, which is equivalent to that

$$0\leq \deg(C'\cdot D_i)\leq \deg(C\cdot D_i),\quad i=0,\dots,r+1. \tag{15}$$

For $i=1,\dots,r$, we have equalities $\deg(C'\cdot D_i)=l_i(\gamma)$ and $\deg(C\cdot D_i)=l_i$. On an other hand, for any $m\in\mathbb{Z}^2$, we have

$$\sum_{i=0}^{r+1}\langle m,\eta_i\rangle\deg(C'\cdot D_i)=\sum_{i=0}^{r+1}\langle m,\eta_i\rangle\deg(C\cdot D_i)=0,$$

since the divisor $\sum_{i=0}^{r+1}\langle m,\eta_i\rangle D_i=\mathrm{div}(t^m)$ is principal. Letting $m=e_1$ and using that $(\eta_{r+1},\eta_0)=(e_1,e_2)$, we deduce that

$$\deg(C'\cdot D_0)=-\sum_{i=1}^{r}\langle e_1,\eta_i\rangle l_i(\gamma),\quad \deg(C\cdot D_0)=-\sum_{i=1}^{r}\langle e_1,\eta_i\rangle l_i,$$

and the same reasonning with $m=e_2$ gives

$$\deg(C'\cdot D_{r+1})=-\sum_{i=1}^{r}\langle e_2,\eta_i\rangle l_i(\gamma),\quad \deg(C\cdot D_{r+1})=-\sum_{i=1}^{r}\langle e_2,\eta_i\rangle l_i.$$

Combined with (15), we deduce that $\gamma\in\Delta_C$, giving an inclusion $V(D)\cap\{0,1\}^{\mathcal{P}}\subset V(E)\cap\{0,1\}^{\mathcal{P}}\cap\Delta_C$.

Let us show the opposite inclusion. If $\gamma\in V(E)\cap\{0,1\}^{\mathcal{P}}\cap\Delta_C$, it lifts to some divisor $C'\in\mathrm{Div}(X)$. By hypothesis, we have $0\leq\gamma\leq\gamma_C$, giving obvious inequalities

$$0\leq\deg(C'\cdot D_i)=l_i(\gamma)\leq l_i=\deg(C\cdot D_i)$$

for all $i=1,\dots,r$. Since $\gamma\in\Delta_C$, we deduce from the previous discussion that (15) holds. Since being nef is equivalent to being globally generated on a toric variety,it follows that both $\mathcal{O}_X(C')$ and $\mathcal{O}_X(C-C')$ are globally generated. By [28], proof of Theorem 2, this gives rise to supplementary vanishing cohomology properties which ensure that C' can be chosen to be an absolute component of C. Since γ is defined over $\mathbb{K}$, such a component is rational by Lemma 8. Thus γ is a $\{0,1\}$-linear combination of the γ_j's, that is $\gamma\in V(D)\cap\{0,1\}^{\mathcal{P}}$. □

Proposition 5 admits the following useful corollary, which is the toric version of [5], Proposition 4.

Corollary 3. *If all the exterior facets of N_f have an inward primitive normal vector with negative coordinates, then $V(E)=V(D)$ if and only if each vector of the reduced echelon basis of $V(E)$ lies in $\{0,1\}^{\mathcal{P}}$.*

Proof. If the reduced echelon basis of $V(E)$ lies in $\{0,1\}^{\mathcal{P}}$, we have $l_i(\gamma)\leq l_i$ for all γ in that basis. By hypothesis, we have $\langle e_k,\eta_i\rangle\leq 0$ for all $i=1,\dots,r$, $k=1,2$ and it follows that $\gamma\in V(E)\cap\{0,1\}^{\mathcal{P}}\cap\Delta_C$. The equality $V(E)=V(D)$ follows from Proposition 5. The other implication is trivial. □

Proposition 5 gives an efficient way to compute the reduced echelon basis of $V(D)$ from the finite set $V(E) \cap \{0,1\}^{\mathcal{P}}$. Roughly speaking, the underlying algorithm is that developed in [28]. It has the advantage to use a smaller lifting precision, but in return, it looks for "good" partitions of $\{0,1\}^{\mathcal{P}}$ and can have an exponential complexity. We don't know what is the probability for that equality $V(E) = V(D)$ holds.

5. Conclusion

We propose a new lifting and recombination algorithm for rational bivariate factorization that takes advantage of the geometry of the Newton polytope. For polynomials that are sparse enough, our complexity is competitive with that of the actual fastest algorithms developed for dense polynomials. We might hope to improve the complexity with a carefull application of the standard modular algorithms in the toric setting.

Acknowledgments. We thank José Ignacio Burgos and Martin Sombra for their careful reading and helpful comments. We thank the anonymous referees for their useful remarks.

References

[1] F. Abu Salem, S. Gao, A.G.B. Lauder, *Factoring polynomials via polytopes*, proc. of ISSAC (2004), pp. 4-11.
[2] M. Andersson, *Residue currents and ideal of meromorphic functions*, Bull. Sci. math. (2004), pp. 481-512.
[3] M. Avendano, T. Krick, M. Sombra, *Factoring bivariate sparse (lacunary) polynomials*, J. of Complexity 23 (2007), pp. 193-216.
[4] K. Belabas, M. Van Hoeij, J. Klüners, A. Steel, *Factoring polynomials over global fields*, J. of Symb. Comp. Vol. 40, Issue 6, pp. 1325-1339 (2005).
[5] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, Proc. of ISSAC 2004, pp 42-49.
[6] L. Busé, G. Chèze, *On the total order of reducibility of a pencil of algebraic plane curves*, Preprint hal-00348561-v.1 (2008).
[7] G. Chèze, *Absolute polynomial factorization in two variables and the knapsack proble*, proc. of ISSAC (2004), pp. 87-94.
[8] G. Chèze and G. Lecerf, *Lifting and recombination techniques for absolute factorization*, J. of Complexity 23, no. 3 (2007), pp. 380-420.
[9] D. Cox, *Toric surfaces*, Lecture 7, Grenoble Summer School 2000 Geometry of toric surfaces.
[10] V. Danilov, *The geometry of toric varieties*, Russian Math. Surveys 33 (1978), pp. 97-154.
[11] M. Elkadi, A. Galligo, M. Weimann, *Towards Toric Absolute Factorization*, J. Symb. Comp. (2008), to appear.
[12] A. Galligo, D. Rupprecht, *Irreducible decomposition of curves*, J. Symb. Comp., 33 (2002), pp. 661-677.
[13] W. Fulton, *Introduction to Toric Varieties*, Annals of Math. Studies, Princeton University Press (1993).
[14] S. Gao, *Factoring multivariate polynomials via partial differential equation*, Math. Comp. 72, no 242 (2003), pp. 801-822.
[15] J. von zur Gathen, J. Gerhard, *Modern computer algebra*, second ed., Cambridge University Press, Cambridge, MA, (2003).
[16] A.G. Khovansky, *Newton polyhedra and toric varieties*, Funct. Anal. Appl. 11 (1977), pp. 56-67.
[17] R. Lazarsfeld, *Positivity in Algebraic Geometry I*, Springer (2005).
[18] G. Lecerf, *New recombination algorithms for bivariate polynomial factorization based on Hensel lifting*, AAECC 21 no. 2 (2010), pp. 151-176.

[19] G. Lecerf, *Sharp precision in Hensel lifting for bivariate polynomial factorization*, Math. of Comp. 75 (2006), pp. 921-933.
[20] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovasz, *Factoring Polynomials with Rational Coefficients*, Math. Ann. 261, no.2 (1982), pp. 515-534.
[21] A. Novocin, *Factoring Univariate Polynomials over the Rationals*, PhD dissertation, Florida State University (2008).
[22] A.M. Ostrowski, *On multiplication and factorization of polynomials. Lexicographic orderings and extreme aggregates of terms*, Aequationes Math. 13 (1975), pp. 201-228.
[23] *Reduzibilität Ebener Kurven*, J. Reine Angew. Math., 369 (1986), pp.167-191.
[24] A. Storjohann, *Algorithms for matrix canonical forms*, PhD thesis, TEH, Zürich (2000). http://www.scg.uwaterloo.ca/~astorjoh.
[25] C. Voisin, *Théorie de Hodge et géométrie algébrique complexe*, SMF (2004).
[26] M. Weimann, *La trace en géométrie projective et torique*, Thèse de l'Université de Bordeaux 1 (2006), http://atlas.mat.ub.es/personals/weimann/Articles.html.
[27] M. Weimann, *An interpolation theorem in toric varieties*, Ann. Inst. Fourier 58, no.4 (2008), pp. 1371-1381.
[28] M. Weimann, *Algebraic osculation and factorization of sparse polynomials*, arXiv 0904.0178v1 (2009).

Departament Algebra i Geometria, Facultat de Matemàtiques, Universitat Barcelona Gran via 585, 08007 Barcelona.

E-mail address: weimann23@gmail.com