Towards Toric Absolute Factorization

M. ELKADI, A. GALLIGO, M. WEIMANN

Université de Nice Sophia Antipolis,
Laboratoire J-A. Dieudonné,
Parc Valrose, 06108 Nice Cedex2, France.

Abstract

This article gives an algorithm to recover the absolute factorization of a bivariate polynomial, taking into account the geometry of its monomials. It is based on algebraic criterions inherited from algebraic interpolation and toric geometry.

1 Introduction

The study of the factorization of a multivariate polynomial f and the production of software dedicated to the effective solving of this problem has received much attention in Computer Algebra. Whereas the rational factorization is only concerned by factors of f in $\mathbb{Q}[\underline{x}] := \mathbb{Q}[x_1, \ldots, x_n]$, the absolute factorization provides all the irreducible factors of f with coefficients in $\overline{\mathbb{Q}}[\underline{x}]$, $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$. For example the polynomial $x_1^2 - 2x_2$ is irreducible in $\mathbb{Q}[x_1, x_2]$, but it has two absolute factors $x_1 - \sqrt{2}x_2$ and $x_1 + \sqrt{2}x_2$.

The bivariate case contains most of difficulties of the multivariate one. In theory, by Bertini's theorem and via Hensel liftings, the multivariate problem reduces to the bivariate one. In the present article we will concentrate on the bivariate case but our techniques naturally extend to n variables case for any $n > 2$.

During more than 30 years of Computer Algebra, the polynomial factorization has been considered from many point of view (see [3, 5, 7] and the references within). In the last decade, two main strategies of absolute polynomial factorization have been quite successful. On the one hand, an algebraic approach relies on the study of Ruppert-Gao matrix [19, 12]. It has been improved in [7, 16] to provide an algorithm with a quasi-optimal complexity. On the other hand, a geometric approach based on a zero-sum criterion (derived from the study of the monodromy group, of a projection of the curve $C := \{a \in \mathbb{C}^2 : f(a) = 0\}$ defined by f on a line, acting on a smooth fiber) provides very efficient semi-numerical probabilistic algorithms able to deal with polynomials having degree up to 200 [20, 4, 5]. A similar strategy was developed and implemented in [22, 23], and its use was extended for obtaining the irreducible decomposition of an algebraic set. The zero-sums considered in [21] admit more general interpretations in Algebraic Geometry as traces.

The aim of this article is first to reinterprete the vanishing traces criterions in the geometric approach as a consequence of Wood's theorem on algebraic interpolation of a family of analytic germs of curves. Second, to provide a generalization of Wood's theorem inspired by [25] and adapted to the factorization of polynomials with fixed Newton polytopes. Third, to outline an algorithm for toric absolute factorization that we experimented successfully on examples.

When the polynomial f of degree d is given by the collection of its coefficients which are all nonzero, its representation is called dense. Whereas when we know that some coefficients of f are zero, we consider its Newton polytope (i.e. the convex hull of exponents of monomials of its nonzero coefficients) and we say that its representation is toric or sparse. Adapted algorithms are developed to take advantage from this representation, e.g. toric elimination received much attention [13, 9].

To our knowledge most of the existing articles on the polynomial factorization deal with dense polynomials, without taking into account the sparseness structure of f. In [1] a study of the toric rational polynomial factorization was presented. It is based on an adapted Hensel lifting. Our aim is to rely on this article, assuming that f is already irreducible in $\mathbb{Q}[\underline{x}]$, and then we compute its absolute factorization. As we shall see in that case, all the Newton polytopes of absolute factors of f are equal and are homothetic to that of f. Hence the combinatorial task is simplified and the difficulty concentrates on the geometry over a fixed toric variety. We mention also [24] where the authors reduce the multivariate sparse factorization to the dense bivariate or univariate polynomial factorization.

The paper is organized as follows. In the next section, we show the special shape of absolute factors of an irreducible rational polynomial. In section 3, we explain the use of interpolation of analytic germes of curves via a Burger's PDE to derive a vanishing trace criteria in $\mathbb{P}^2(\mathbb{C})$, and we recall the use of monodromy action. In section 4 we provide a generalization of this trace criteria to a (possibly singular) toric surface. In section 5 we outline an algorithm for toric absolute factorization. It is based on algebraic criterions inherited from interpolation problems in toric geometry, and computations of traces. It generalizes and improves the algorithm developed for dense polynomials in [20, 5]. Then we illustrate its different steps on an example. We finish with concluding remarks and future improvements. At the end of this paper a short Appendix collects some properties on abstract toric surfaces needed for our developments.

Hereafter $\mathbb{P}^n$ denotes the projective space over $\mathbb{C}$ of dimension n. For a polynomial map (f, q) in $\mathbb{C}^2$, $\mathrm{Jac}(f, q)$ is its jacobian. The Newton polytope of a polynomial f is denoted by N_f. We denote the mixed volume of two polytopes P and Q by $\mathrm{MV}(P, Q)$.

2 Factorization and Newton polytopes

We recall that the Minkowski sum of two polytopes P and Q is

$$P + Q = \{p + q : p \in P, q \in Q\}.$$

The crucial observations for our purpose are the following two results.

Proposition 1 *(Ostrowksi theorem [18]) The Newton polytope of the product of two polynomials g and h is the Minkowski sum of Newton polytopes of its factors: $N_{gh} = N_g + N_h$.*

So if the irreducible polynomial $f \in \mathbb{Q}[\underline{x}]$ has a polytope which is integrally indecomposable, f is absolutely irreducible. For a study of the irreducibility of a polynomial from the Newton polytope point of view, see [11].

Proposition 2 *Let $f \in \mathbb{Q}[\underline{x}]$ be an irreducible polynomial and $f = f_1 \dots f_q$ be its absolute factorization. Then the irreducible absolute factors f_i of f are conjugate over $\mathbb{Q}$.*

Proof. Up to a linear change of coordinates, we can assume that f is monic in x_2, and consequently its absolute factors are also monic in x_2. Let G be the Galois group of the smallest extension of $\mathbb{Q}$ containing all the coefficients of f_1. If $\sigma \in G$, the conjugate polynomial $\sigma(f_1)$ of f_1 also divides f. Now as f is an irreducible element in $\mathbb{Q}[\underline{x}]$, the polynomial $\prod_{\sigma \in G} \sigma(f_1) = f$, and so each absolute factor f_j of f is equal to $\sigma(f_1)$ for some $\sigma \in G$. $\square$

The determination of Newton polytopes of absolute factors of an irreducible polynomial in $\mathbb{Q}[\underline{x}]$ is highly simplified by the following corollary.

Corollary 1 *Let $f \in \mathbb{Q}[\underline{x}]$ be an irreducible polynomial and $f = f_1 \dots f_q$ be its absolute factorization. Then $N_{f_1} = \cdots = N_{f_q}$ and $N_f = qN_{f_1}$.*

Remark 1 For instance, a polynomial $f \in \mathbb{Q}[x]$ of bidegree (d_1, d_2) which is irreducible over $\mathbb{Q}$ is irreducible over $\mathbb{C}$ if d_1 and d_2 are relatively prime.

Proposition 2 implies in particular that the irreducible rational polynomial f has no multiple factor over $\mathbb{C}$.

Another important algorithmic consequence of Proposition 2 is that the absolute factorization of f is completely determined by the number of factors q, an irreducible univariate polynomial $g(t) \in \mathbb{Q}[t]$ defining a finite extension $\mathbb{K} = \mathbb{Q}[t]/\big(g(t)\big)$, and the coefficients of f_1 which belong to $\mathbb{K}$ and are indexed by the lattice points in the polytope $\frac{1}{q}N_f \subset \mathbb{N}^2$.

3 Factorization and Algebraic Interpolation

Let f be an irreducible bivariate rational polynomial of total degree d. Since f is reduced over $\mathbb{C}$, its absolute irreducible factors are in one-to-one correspondence with irreducible components of the affine curve C defined by f:

$$C = \{(x_1, x_2) \in \mathbb{C}^2 : f(x_1, x_2) = 0\}.$$

Sard-Bertini theorem combined with Bézout's theorem ensure that for $t = [t_0 : t_1 : t_2]$ generic in the dual projective space $(\mathbb{P}^2)^*$, the affine line

$$L_t = \{(x_1, x_2) \in \mathbb{C}^2 : t_0 + t_1 x_1 + t_2 x_2 = 0\}$$

intersects C transversely in d distinct points whose coordinates vary holomorphically with t by the implicit function theorem. Thus L_t defines a degree d reduced 0-cycle of C:

$$L_t \cdot C = p_1(t) + \cdots + p_d(t).$$

The principle of unicity of analytic continuation and Bézout's theorem imply that f admits a factor of degree $k \leq d$ if and only if there exists

$$I = \{i_1, \dots, i_k\} \subset \{1, \dots, d\}$$

and an algebraic curve $C_I \subset \mathbb{C}^2$ of degree k such that (as shown in Figure 1) for t in a small open set of $(\mathbb{P}^2)^*$:

$$L_t \cdot C_I = p_{i_1}(t) + \cdots + p_{i_k}(t).$$

Hence, we are brought to consider the following question: let $t \in (\mathbb{P}^2)^*$ distinct

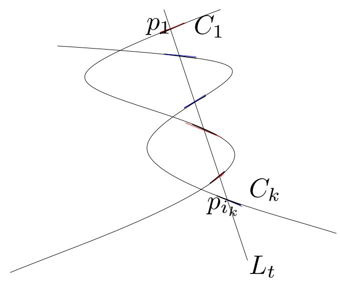

Figure 1:

from the point at infinity $[1:0:0]$ and let $C_1 \cup \ldots \cup C_k$ be an union of germs of smooth analytic curves (algebraic in our case) of $\mathbb{C}^2$ transverse to the line L_t at pairwise distinct points $p_1(t), \ldots, p_{i_k}(t)$. Does there exist an algebraic curve of total degree k which contains all these germs C_i ?

The following result solves precisely this problem.

Theorem 1 *(Wood's theorem [26]) The union of analytic curves $C_1 \cup \ldots \cup C_k$ is contained in an algebraic curve of degree k if and only if the germ of holomorphic function trace on the first coordinate defined by*

$$(Tr\, x_1)(t) := \sum_{i=1}^{k} x_1(p_{i_j}(t))$$

is affine in the constant coefficient t_0 of L_t.

Geometrically, this result asserts that an analytic curve is algebraic if and only if the barycenters of intersection points with a generic line L lie on a line (called a diameter of the curve, see the line D in Figure 2) when L moves parallel to itself, as shown in Figure 2. Newton had already remarked in [17] this property for algebraic plane curves of degree 3. The proof of Theorem 1 in [26] is simple but relies on a tricky use of a Burger's PDE. It will be generalized for our purpose in section 4.

In [20, 5] an algorithm for absolute dense factorization was developed based on vanishing partial sums. This algorithm uses topological considerations about the complex plane $\mathbb{C}^2$. Its proof relies on Harris uniform position theorem and Van Kampen theorem which establish the link between the irreducibility of an affine algebraic curve and the transitive action of a monodromy group (see [5] for details). It turns out that this condition on vanishing partial sums is equivalent to the interpolation criterion given by Wood's theorem. Let us recall briefly the principle of this method. Up to a linear change of variables, we assume that f is monic as a polynomial in x_2 of degree d. For $x_1 = a$ generic, let

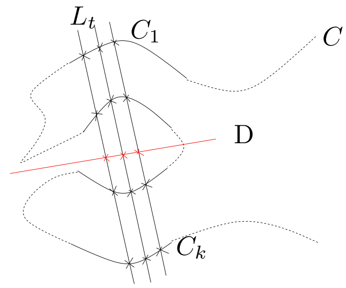

Figure 2:

$x_{2,1}(a), \ldots, x_{2,d}(a)$ be the roots of the univariate polynomial $f(a, x_2)$. For each $i = 1 \ldots d$, let

$$\phi_i(x_1) = \sum_j \alpha_{j,i}(a)(x_1 - a)^j$$

be the power series satisfying $\phi_i(a) = x_{2,i}(a)$ and $f\big(x_1, \phi_i(x_1)\big) = 0$. Then $f(x) = f(x_1, x_2) = \prod_{i=1}^d \big(x_2 - \phi_i(x_1)\big)$. Every absolute factor of f has the form

$$f_I = \prod_{i \in I} \big(x_2 - \phi_i(x_1)\big) = x_2^\delta + a_{I,1}(x_1)x_2^{\delta-1} + \cdots + a_{I,\delta}(x_1),$$

with $I \subset \{1, \ldots, d\}, \mathrm{card}(I) = \delta$ and $\deg a_{I,i}(x_1) \leq i$ for $i = 1 \ldots \delta$. In particular, the degree of $a_{I,1}(x) = -\sum_{i \in I} \phi_i(x_1)$ is at most 1, then $\sum_{i \in I} \alpha_{2,i}(a) = 0$. Because of the genericity, it turns out that this last condition is also sufficient for f to have an absolute factor. So in order to find absolute factorization of f it suffices to search minimal zero sums between the complex numbers $\alpha_{2,1}(a), \ldots, \alpha_{2,d}(a)$.

The brute force resulting algorithm requires 2^d trace tests to detect factors of f. Strategies relying on LLL were developed and implemented in [4] to decrease this high number of tests.

4 Interpolation in toric surfaces

In [25] a necessary and sufficient condition was given for a family of germs of analytic hypersurfaces in a smooth projective toric variety X to be interpolated by an algebraic hypersurface with a prescribed class in the Chow ring of X. Here we establish a similar result in a toric surface which can be singular. It will be useful for our approach to the absolute factorization problem.

4.1 Toric surfaces

Let us denote by $\mathbb{T}$ the algebraic torus $(\mathbb{C}^*)^2$. The Newton polytope P of a Laurent polynomial f gives information about the asymptotic behavior of the curve

$$C := \{x \in \mathbb{T},\ f(x) = 0\}.$$

For example, if f is not identically zero for $x_1 = 0$, C meets (asymptotically) the divisor $x_1 = 0$ in d points (taken into account multiplicities), where d is the number of integer points of the facet $(\{0\} \times \mathbb{R}^+) \cap P$.

We say that a curve $D \subset \mathbb{T}$ is supported by an integer convex polyope Q if it is the zero set of a Laurent polynomial with Newton polytope Q.

Let Q be an integer convex polytope such that $Q \cap \mathbb{Z}^2 = \{m_0, \ldots, m_l\}$. Consider the morphism

$$\begin{array}{rcl} \phi_Q : \mathbb{T} & \longrightarrow & \mathbb{P}^l \\ x = (x_1, x_2) & \longmapsto & [x^{m_0} : \cdots : x^{m_l}]. \end{array}$$

The Zariski closure X_Q of $\phi_Q(\mathbb{T}) \subset (\mathbb{C}^*)^l$ in $\mathbb{P}^l$ is the projective toric variety associated to Q. See [10] or Appendix at the end of this paper where the definition of an abstract toric surface and some of their properties are provided.

Without lost of generality we assume that $m_0 = 0$. The following Lemma will be useful.

Lemma 1 *We have* $\dim X_Q = \dim Q$*. If* $\dim Q = 2$*, the map* ϕ_Q *is an injective immersion if and only if the gcd of integers* $d_{k,p} = \det(m_k, m_p)$*,* $1 \leq k, p \leq l$*, is equal to* 1*. In particular, this is the case if the finite set* $Q \cap \mathbb{Z}^2 = \{m_1, \ldots, m_l\}$ *generates the free* $\mathbb{Z}$*-module* $\mathbb{Z}^2$*.*

Proof. For $k = 1 \ldots l$, let $m_k = (m_{k1}, m_{k2})$. If $x = (x_1, x_2)$ and $y = (y_1, y_2)$ are in $\mathbb{T}$,

$$\begin{array}{rl} & \phi_Q(x) = \phi_Q(y) \Longleftrightarrow [1 : x^{m_1} : \cdots : x^{m_l}] = [1 : y^{m_1} \cdots : y^{m_l}] \\ \Longleftrightarrow & \forall k, p = 1 \ldots l, \left(\dfrac{x_1}{y_1}\right)^{m_{k1}m_{p2} - m_{k2}m_{p1}} = \left(\dfrac{x_2}{y_2}\right)^{m_{k1}m_{p2} - m_{k2}m_{p1}} = 1. \end{array}$$

Thus the complex numbers $c_i := \frac{x_i}{y_i}$, $i = 1, 2$ satisfy $c_i^{d_{k,p}} = 1$ and $c_1 = c_2 = 1$ if and only if the greatest common divisor of the integers $d_{k,p}$, $1 \leq k, p \leq l$ is 1. In particular, this is the case if there exist two vectors m_k and m_p such that $\det(m_k, m_p) = 1$. Moreover, the minor $M_{k,p}(\phi_Q)$ of the jacobian matrix of ϕ_Q corresponding to m_k and m_p is equal to

$$M_{k,p}(\phi_Q) = (m_{1k}m_{2p} - m_{1p}m_{2k})x^{m_k + m_p - (1,1)},$$

so that ϕ_Q has rank two (on $\mathbb{T}$) if and only if $\dim Q = 2$. $\square$

Remark 2 This proof also shows that ϕ_Q is an N-to-one map on its image, where $N = [\mathbb{Z}^2 : M_Q]$ is the index of the lattice M_Q generated by $Q \cap \mathbb{Z}^2$ in the lattice $\mathbb{Z}^2$.

4.2 Traces for curves in toric surfaces

4.2.1 Notations

Here we set notations that we will keep in the sequel of the paper.

Let $Q \subset \mathbb{R}^2$ be a 2-dimensional integer convex polytope with lattice points $m_0 = 0, m_1, \ldots, m_l$. We assume that Q satisfies the assumption:

$$\mathbb{Z}^2 \text{ is generated on } \mathbb{Z} \text{ by } \{m_1, \ldots, m_l\}. \tag{1}$$

The convex polytopes Q which do not satisfy this property are rare and have a very special shape.

Let $X = X_Q$ be the projective toric surface associated to Q, and $[u_0 : \cdots : u_l]$ be homogeneous coordinates on $\mathbb{P}^l$. Every Laurent polynomial

$$q_a(x) = \sum_{i=0}^{l} a_i x^{m_i}$$

supported by Q determines a curve $C_a := \{q_a = 0\} \subset \mathbb{T}$. Since ϕ_Q is assumed to be one-to-one (Lemma 1), by Lemma 3 in Appendix, for a generic, C_a can be identified with the hyperplane section of $X \cap (\mathbb{C}^*)^l$ defined by the projective hyperplane

$$H_a = \{u \in \mathbb{P}^l : \sum_{i=0}^{l} a_i u_i = 0\}.$$

We denote by $a = [a_0 : \cdots : a_l]$ the point of the dual space $(\mathbb{P}^l)^*$ corresponding to C_a.

For the definition of the mixed volume in the following lemma and its properties, see [13].

Lemma 2 *Let $C \subset \mathbb{T}$ be a reduced curve supported by a lattice polytope P. For $a \in (\mathbb{P}^l)^*$ generic, C_a is smooth, irreducible and intersects C transversely in $d = \mathrm{MV}(P, Q)$ distinct points $p_1(a), \ldots, p_d(a)$, where $\mathrm{MV}(P, Q)$ denotes the mixed volume of (P, Q).*

Proof. Let us denote by $\mathcal{C}$ and $\mathcal{C}_a$ the Zariski closure in X of the affine curves $\phi_Q(C)$ and $\phi_Q(C_a)$. We know from Lemma 3 in Appendix that $\mathcal{C}_a$ coincides for generic a with the hyperplane section $H_a \cap X$ of X. Thus Bertini's theorem implies that the curve $\mathcal{C}_a$ is generically smooth irreducible and intersects $\mathcal{C}$ in its Zariski open set $\phi_Q(C)$. Since by Lemma 1 ϕ_Q is an embedding, we deduce that C_a is generically smooth, irreducible and intersects C transversely in $d = \deg(H_a \cdot X \cdot \mathcal{C})$ points. Bernstein's theorem asserts that this degree $d = \deg\big(\mathcal{O}_X(1)\big)_{|\mathcal{C}} = \mathrm{MV}(P, Q)$. □

From this lemma, we have the following definition.

Definition 1 *For any holomorphic function h near $C_\alpha \cap C$, the trace of h on C relatively to the polytope Q is*

$$(\mathrm{Tr}_C h)(a) := \sum_{j=1}^{d} h(p_j(a)).$$

This function is defined and holomorphic for a near α.

4.2.2 A necessary condition to interpolate germs of curves

We provide a necessary condition for a family of germs of curves to be interpolated by an algebraic curve C.

Since $m_0 = 0$ is a vertex of the polytope Q, the generic polynomial q_a has a nonzero constant term a_0.

Theorem 2 *Let $C \subset \mathbb{T}$ be an algebraic curve, and $\alpha \in (\mathbb{P}^l)^*$ satisfying the hypothesis of Lemma 2. We denote by Γ the union of facets of Q not containing 0. For $n \in \mathbb{N}^*$ and $s \in n(Q \cap \mathbb{Z}^2)$, we have*

$$\begin{aligned} \partial_{a_0}^{(n)}\big(\mathrm{Tr}_C\, x^s\big) &= 0 \quad \text{if} \quad s \in n(Q \setminus \Gamma), \\ \partial_{a_0}^{(n+1)}\big(\mathrm{Tr}_C\, x^s\big) &= 0 \quad \text{if} \quad s \in n\Gamma. \end{aligned} \tag{2}$$

Proof. Suppose that $C = \{f = 0\}$, for a Laurent polynomial $f = \sum c_m x^m$. The trace function $\mathrm{Tr}_C\, x^s$ is a rational function on $\mathbb{P}^l$, it is homogeneous of degree 0 in a. If we denote by res_p and Res respectively the local Grothendieck residues at p and the global Grothendieck residue (see [14], §5), then for a in a small neighborhood of α,

$$\big(\mathrm{Tr}_C\, x^s\big)(a) = \sum_{p \in \mathbb{T}} \mathrm{res}_p \frac{x^s df \wedge dq_a}{f q_a} = \mathrm{Res}\begin{bmatrix} x^s df \wedge dq_a \\ f \quad q_a \end{bmatrix}. \tag{3}$$

Since

$$df \wedge dq_a = \Big(\sum_{(m,m_i)} a_i\, c_m \det(m, m_i) x^{m+m_i-(1,1)} \Big)\, dx_1 \wedge dx_2,$$

we obtain

$$\big(\mathrm{Tr}_C\, x^s\big)(a) = \sum_{(m,m_i)} a_i\, c_m \det(m, m_i)\ \mathrm{Res}\begin{bmatrix} x^{s+m+m_i} \frac{dx_1 \wedge dx_2}{x_1 x_2} \\ f \quad q_a \end{bmatrix}. \tag{4}$$

Using Cauchy formula for residues and Stokes theorem [14],

$$\partial_{a_0}^{(n)}\left(\mathrm{Res}\begin{bmatrix} x^{s+m+m_i} \frac{dx_1 \wedge dx_2}{x_1 x_2} \\ f \quad q_a \end{bmatrix} \right) = (-1)^n\, n!\, \mathrm{Res}\begin{bmatrix} x^{s+m+m_i} \frac{dx_1 \wedge dx_2}{x_1 x_2} \\ f \quad q_a^{n+1} \end{bmatrix}. \tag{5}$$

If P^0 denotes the interior of a polytope P, then by the toric version of Abel-Jacobi theorem [15], we have

$$s + m + m_i \in \big(N_f + (n+1)Q\big)^0 \implies \mathrm{Res}\begin{bmatrix} x^{s+m+m_i} \frac{dx_1 \wedge dx_2}{x_1 x_2} \\ f \quad q_a^{n+1} \end{bmatrix} = 0, \tag{6}$$

where N_f is the Newton polytope of f.

Let us denote by $Q_1 = [0, s_1]$ and $Q_2 = [0, s_2]$ the two facets of Q containing the origin 0, so that $Q = Q^0 \cup Q_1 \cup Q_2 \cup \Gamma$. To finish the proof we consider different cases:

1. If $s \in (nQ)^0$, then for all $m \in N_f$ and $m_i \in Q$,

   $s + m + m_i \in \big(N_f + (n+1)Q\big)^0$, so that $\partial_{a_0}^{(n)}(\mathrm{Tr}_C\, x^s) = 0$.

2. Let $s \in Q_1 \setminus \{ns_1\} = [0, ns_1[$. Since we are dealing with residues in the torus, we check easily that (3) depends on f up to multiplication by any Laurent monomial. Thus we can assume that N_f is contained in the cone generated by Q and intersects the ray $\mathbb{R}^+ s_1$ in a non empty set $N \subset N_f$ (consisting in one vertex or one facet of N_f). In this case, it is easy to check that for all $m \in N_f$ and $m_i \in Q$ such that $m + m_i \notin \mathbb{R}^+ s_1$,

$s+m+m_i \in \big(N_f+(n+1)Q\big)^0$. Moreover, $m+m_i \in \mathbb{R}^+ s_1$ if and only if m and m_i are in $\mathbb{R}^+ s_1$, that is $\det(m, m_i)=0$. The formulas (4) and (6) show that $\partial_{a_0}^{(n)}(\mathrm{Tr}_C\, x^s)=0$.

The same argument hols for $s \in [0, ns_2[$.

3. If $s \in n\Gamma \setminus \{ns_1, ns_2\}$, N_f is contained in the cone $\mathbb{R}^+ Q$ and we check that for all $m_i \in Q$ and $m \in N_f$, $s+m+m_i \in \big(N_f+(n+2)Q\big)^0$, so $\partial_{a_0}^{(n+1)}(\mathrm{Tr}_C\, x^s)=0$.

4. Let $s = ns_1$, as for the case 2, we choose $N_f \subset \mathbb{R}^+ Q$ such that $N = N_f \cap \mathbb{R}^+ s_1$ is non empty. Then we check easily that if m or m_i does not belong to $\mathbb{R}^+ s_1$, $s+m+m_i \in \big(N_f+(n+2)Q\big)^0$ and if m and m_i are in $\mathbb{R}^+ s_1$, $\det(m, m_i)=0$. So when $s = ns_1$, $\partial_{a_0}^{(n+1)}(\mathrm{Tr}_C\, x^s)=0$.

   The same argument is valid for $s = ns_2$.

These items combined with (4), (5) and (6) imply (2).

□

4.3 Criterion for algebraic interpolation

Now we give a necessary and sufficient criterion of interpolation generalizing Theorem 1 to our setting. Recall that Q satisfies the condition (1). To simplify the exposition and without lost of generality we further assume that the vectors $m_1 \in Q$ and $m_2 \in Q$ generate the lattice $\mathbb{Z}^2$ and $a_1, \dots, a_t$ code the vertices of Q other than 0. Hence $a_{t+1}, \dots, a_l$ code the other points of Q, where $l = \mathrm{card}(Q \cap \mathbb{Z}^2) - 1$.

Theorem 3 *Let $\alpha \in (\mathbb{P}^l)^*$ such that $C_a \subset \mathbb{T}$ is an irreducible smooth curve supported by Q for any a near α. Let*

$$C = C_1 \cup \cdots \cup C_d$$

be an union of germs of smooth analytic curves at pairwise distinct points $p_1, \dots, p_d$ of C_α. Suppose that none of the germs C_i is contained in a curve $\{x^{m_1} - c = 0\}$, $c \in \mathbb{C}^*$. Then, there exists an algebraic curve $\widetilde{C} \subset \mathbb{T}$, containing C and supported by a polytope P whose mixed volume with Q is d, if and only if, for generic $(a_1, \dots, a_l)$ in a neighborhood of $(\alpha_1, \dots, \alpha_l)$, the germ of holomorphic function

$$a_0 \quad \longmapsto \quad \big(\mathrm{Tr}_C\, x^{m_1}\big)(a_0)$$

is polynomial of degree at most 1 in the constant coefficient a_0.

Proof. Suppose that $\widetilde{C} = \{f = 0\}$, where f is a Laurent polynomial with Newton polytope P such that $\mathrm{MV}(P, Q) = d$. As $C \subset \widetilde{C}$, the two sets $C \cap C_a$ and $\widetilde{C} \cap C_a$ coincide for a in a sufficiently small neighborhood $U_\alpha \subset (\mathbb{P}^l)^*$ of α, since by Lemma 2 they have the same cardinal $d = \mathrm{MV}(P, Q)$. Thus, for $a \in U_\alpha$,

$$\forall\, s \in \mathbb{Z}^2,\ \mathrm{Tr}_C\, x^s = \mathrm{Tr}_{\widetilde{C}}\, x^s,$$

and the necessary condition follows from Theorem 2.

Conversely, since the curve C_α is supported by Q, none of the coefficients $(\alpha_0,\dots,\alpha_t)$ vanish.

Let us denote by $p_j(a)$ the intersection point of the germ C_j at α with C_a and we define the following germs of holomorphic function at $\alpha\in(\mathbb{P}^l)^*$

$$X_i^{(j)}(a) := x^{m_i}(p_j(a)),\quad i=0\dots l,\quad j=1\dots d.$$

We have

$$y\in C_j\cap C_a \Longrightarrow X_i^{(j)}(-\sum_{i=1}^{l} a_i y^{m_i}, a_1,\dots,a_l) = y^{m_i}, \forall a\in U_\alpha, \tag{7}$$

where U_α is a neighborhood of α. Differentiating the right side of this implication according to a_1, we obtain:

$$\big(\partial_{a_1}X_i^{(j)} - y^{m_1}\partial_{a_0}X_i^{(j)}\big)\big(-\sum_{i=1}^{l} a_i y^{m_i}, a_1,\dots,a_l\big) = 0.$$

Replacing $y\in C_j$ by $p_j(a)\in C_j$, and using the equality $-\sum_{i=1}^{l} a_i y^{m_i}\big(p_j(a)\big) = a_0$, we obtain a Burger's PDE:

$$\partial_{a_1}X_i^{(j)}(a) - X_1^{(j)}(a)\partial_{a_0}X_i^{(j)}(a) = 0.$$

So for $i=1$,

$$\partial_{a_1}X_1^{(j)} = \frac{1}{2}\partial_{a_0}\big[X_1^{(j)}\big]^2.$$

This PDE is summable on j and gives rise, to

$$\partial_{a_1}\big(\mathrm{Tr}_C\, x^{m_1}\big) = \frac{1}{2}\partial_{a_0}\big(\mathrm{Tr}_C\, x^{2m_1}\big).$$

We have a propagation of the behavior in the variable a_0: if $\mathrm{Tr}_C\, x^{m_1}$ is affine in a_0 then obviously $\partial_{a_1}(\mathrm{Tr}_C\, x^{m_1})$ is affine in a_0. By this PDE, $\partial_{a_0}(\mathrm{Tr}_C\, x^{2m_1})$ is also affine in a_0, hence the degree of $\mathrm{Tr}_C\, x^{2m_1}$ in a_0 equals at most 2. By induction on n, the map

$$a_0 \mapsto \mathrm{Tr}_C\, x^{nm_1}$$

is a polynomial of degree at most n in a_0.

Consider the following polynomial in X:

$$\begin{aligned} P(X,a) &:= \big(X - X_1^{(1)}(a)\big)\times\cdots\times\big(X - X_1^{(d)}(a)\big) \\ &= X^d - \sigma_1(a)X^{d-1} + \cdots + (-1)^d\sigma_d(a), \end{aligned}$$

the σ_i's are the elementary symmetric functions of $x^{m_1}\big(p_1(a)\big),\dots,x^{m_1}\big(p_d(a)\big)$. Replacing a_0 by $-\sum_{i=1}^{l} a_i x^{m_i}$, and denoting $a' := (a_1,a_2,\dots,a_l)$ and $a" = (a_1,\dots,a_t)$, we obtain a function

$$Q_{a'}(x) = \big(x^{m_1} - X_1^{(1)}(-\sum_{i=1}^{l} a_i x^{m_i}, a')\big)\times\cdots\times\big(x^{m_1} - X_1^{(d)}(-\sum_{i=1}^{l} a_i x^{m_i}, a')\big)$$

which vanishes on C for any a' near α', using (7).

Now, Newton formulas relating the coefficients of P with the traces of the power of the Laurent monomial x^{m_1} imply that the analytic functions

$$(a_0, a'') \mapsto \sigma_i(a_0, a'', \alpha_{t+1}, \dots, \alpha_l)$$

are polynomial in a_0 (with degree at most n) for any $a'' := (a_1, \dots, a_t)$ near α''. Thus the function

$$R_{a''}(x) := Q_{a'', \alpha_{t+1}, \dots, \alpha_l}(x)$$

is a Laurent polynomial in x vanishing on C. So that the algebraic set defined by the following infinite numbers of equations:

$$\widetilde{C} := \{x \in \mathbb{T} : R_{a''}(x) = 0, \forall\, a'' \text{ near } \alpha''\}$$

contains C. We need to show that $C_a \cap \widetilde{C} = \{p_1(a), \dots, p_d(a)\}$ for all a in a neighborhood of α. By construction, a point q belongs to $\widetilde{C} \cap C_\alpha$ if and only if there exists $j \in \{1, \dots, d\}$ such that for all a'' near α''

$$x^{m_1}(q) = x^{m_1}\big(p_j(-a_1 x^{m_1}(q) - a_2 x^{m_2}(q) - \sum_{i=3}^{l} \alpha_i x^{m_i}(q), a_1, a_2, \alpha_3 \dots, \alpha_l)\big). \quad (8)$$

Let us suppose that C_j is locally parameterized by

$$C_j = \{p(t),\ |t| < \epsilon,\ p(0) = p_j\}.$$

We consider the affine system in (a_0, a_2):

$$\begin{cases} a_0 + \alpha_1 x^{m_1}\big(p(t)\big) + a_2 x^{m_2}\big(p(t)\big) = c_p \\ a_0 + \alpha_1 x^{m_1}(q) + a_2 x^{m_2}(q) = c_q \end{cases} \quad (9)$$

where we define $c_q := -\sum_{i=3}^{l} \alpha_i x^{m_i}(q)$ for any $q \in \mathbb{T}$. Suppose that there exists $q \in C_\alpha \setminus \{p_j\}$ which satisfies (8). Then $x^{m_1}(q) = x^{m_1}(p_j)$ and, since m_1 and m_2 generate $\mathbb{Z}^2$, $q \neq p_j$ implies $x^{m_2}(q) \neq x^{m_2}(p_j)$. Thus, it is easy to check that there is an unique solution $(a_0(t), a_2(t))$ to (9) which converges to (α_0, α_2) when $|t|$ goes to zero. Thus, the map

$$a_2 \longmapsto p_j\big(-\alpha_1 x^{m_1}(q) - a_2 x^{m_2} - \sum_{i=3}^{l} \alpha_i x^{m_i}(q), \alpha_1, a_2, \alpha_3, \dots, \alpha_l\big)$$

is surjective from a neighborhood of α_2 to C_j, so that

$$x^{m_1}(q) = x^{m_1}(p),\ \ \forall\ p \in\ C_j.$$

This situation has been excluded by hypothesis. Thus we have proved that

$$\widetilde{C} \cap C_\alpha = C \cap C_\alpha.$$

By hypothesis, the last reasoning is valid when replacing $(\alpha_0, \dots, \alpha_t)$ by a vector in its neighborhood. Thus for $(a_0, a")$ close to $(\alpha_0, \alpha")$

$$\widetilde{C} \cap C_{a_0, a", \alpha_{t+1}, \dots, \alpha_l} = C \cap C_{a_0, a", \alpha_{t+1}, \dots, \alpha_l}.$$

Since the coefficients $(a_0, a_3, \ldots, a_t)$ correspond to the vertices of Q, the Zariski closure of $C_{a_0,a",\alpha_{t+1},\ldots,\alpha_l}$ in the toric variety $X = X_Q$ can avoid any finite subset of the divisor at infinity $X \setminus \mathbb{T}$ by choosing a generic value of $(a_0, a")$. Thus the Zariski closure in X of the two curves $\widetilde{C}$ and $C_{a_0,a",\alpha_{t+1},\ldots,\alpha_l}$ intersect transversely in the torus for $a"$ generic. This open condition remains valid for any a in a neighborhood of α so that for all a near α, $\widetilde{C} \cap C_a = \widetilde{C} \cap C_\alpha$. By Lemma 2, $\widetilde{C}$ is supported by a polytope P whose mixed volume with Q is d.

□

5 Algorithm for toric absolute factorization

We describe an algorithm for the absolute factorization of a bivariate irreducible polynomial $f \in \mathbb{Q}[x]$ with Newton polytope P.

We denote by $X = \mathbb{T} \cup D_1 \cdots \cup D_r$ the abstract toric variety associated to P, where the divisor D_i corresponds to the facet P_i of P (see Appendix or [10]). We assume that the origin is a vertex and that P_1 and P_2 contain it.

Algorithm:
Input: A bivariate irreducible polynomial $f \in \mathbb{Q}[x]$.
Output: The absolute irreducible decomposition of f (i.e. its irreducible factorization in $\mathbb{C}[x]$).

1. Determine the representation of P as intersection of affine half-planes:

$$P = \{m \in \mathbb{R}^2,\ \langle m, \eta_i \rangle + k_i \geq 0,\ i = 1 \ldots r\}$$

   such that $P_i = \{m \in Q, \langle m, \eta_i \rangle + k_i = 0\}$, $i = 1 \ldots r$, support the facets of P.

2. Find the smallest integer polytope Q such that $P = dQ$, $d \in \mathbb{N}^*$. Let q be a generic Laurent polynomial supported by Q, and for $t \in \mathbb{C}$ generic, we denote by $C_t \subset X$ the curve defined by $q(x) - t$. Determine the 0-cycle $C_t \cdot C = p_1(t) + \cdots + p_N(t)$ on X.

3. For each $i = 3 \ldots r$, determine the set $C \cdot D_i = \{p_{i1}, \ldots, p_{il_i}\}$ (each p_{ij} is repeated according to its multiplicity).

4. Find the unique partition of $\{1, \ldots, N\}$

$$\mathcal{J} := (J_{31} \cup \cdots \cup J_{3l_3}) \cup \cdots \cup (J_{r1} \cup \cdots \cup J_{rl_r})$$

   such that $\mathrm{card}(J_{ik}) = k'_i = \frac{k_i}{d} \in \mathbb{N}$ and $\lim_{|t| \to \infty} p_j(t) = p_{ik} \Longleftrightarrow j \in J_{ik}$.

5. Find the biggest divisor δ of d such that for each $i = 3 \ldots r$, there exists $J_i \subset \{1, \ldots, l_i\}$ of cardinal $\frac{l_i}{\delta}$ satisfying

$$T_{\delta,J_3,\ldots,J_r} := \sum_{i=3}^{r} \sum_{k \in J_i} \sum_{j \in J_{ik}} \frac{f_{x_2}}{\mathrm{Jac}(f,q)}\big(p_j(t)\big) = 0. \qquad (10)$$

6. Theorem 1 implies that f admits δ absolute irreducible factors whose traces on the facets $P_3, \dots, P_3$ are given by the partition $\mathcal{J}$. Explicit these factors using Hensel's liftings as in [1] but with approximate coefficients as in [5, 20].

7. From the approximate factorization, compute the extension $\mathbb{K}$ in section 2 and recognize the exact factorization as explained in [5, 6].

Remark 3 Before the proof of the algorithm, let us give some remarks and comments on some of these different points.

Our main target is not polynomials with too small polytopes (which can be treated by other means), so we assume that $(1,0)$ is not a vertex of Q.

The curve $C \subset X$ determined by f belongs to the linear system $|D_P| = |dD_Q|$, where $D_Q = k'_3 D_3 + \cdots + k'_r D_r$.

The number of points N in the cycle $C_t \cdot C$ is equal by Bernstein's theorem to $d(D_Q \cdot D_Q) = 2d\mathrm{vol}(Q)$ (see [2]). The curve $C_t \subset X$ is the zero set of the homogeneous polynomial $Q^h(U) - t\prod_{i=3}^r U_i^{k'_i}$, where $U = (U_1, \dots, U_r)$ are homogeneous coordinates on X associated to the edges of Q and Q^h is the Q-homogeneization of q (see [8]). When $|t|$ goes to infinity, C_t degenerates to the effective divisor at infinity $D_Q = \mathrm{div}_0(\prod_{i=3}^r U_i^{k'_i})$, and

$$p_1(t) + \cdots + p_N(t) \longrightarrow k'_3(p_{31} + \cdots + p_{3l_3}) + \cdots + k'_r(p_{r1} + \cdots + p_{rl_r}).$$

In the examples, to determine the partition of $\{1, \dots, N\}$ in the algorithm, we fix t with $|t|$ big and we solve the polynomial system $f = q - t = 0$.

Proof of the algorithm. Let d' be a divisor of d and set $N' := \frac{N}{d'} = 2\frac{d}{d'}\mathrm{vol}(Q)$. To any subset $J = \{j_1, \dots, j_{N'}\}$ of $\{1, \dots, N\}$, we associate the 0-cycle

$$p_{j_1}(t) + \cdots + p_{j_{N'}}(t).$$

Since $(1,0) \notin \Gamma$ (Γ is defined in Theorem 2), and absolute irreducible factors of f are supported by a polytope homothetic to Q, the curve $C = \{f = 0\}$ intersects properly the Zariski closure of any line $x_1 = c$, $c \in \mathbb{C}$. Thus, Theorem 2 and Theorem 3 imply that there exists an algebraic curve $C_J \subset X$ such that for any $t \in \mathbb{C}$,

$$C_J \cdot C_t = p_{j_1}(t) + \cdots + p_{j_{N'}}(t)$$

if and only if the trace of x_1

$$T_J(t) := x_1(p_{j_1}(t)) + \cdots + x_1(p_{j_{N'}}(t))$$

does not depend on t. Such a curve is contained in C and is supported by $(d/d')Q$. If d' is the biggest divisor of d for which there exists a vanishing sum as in (10), $C_J = C_J(d')$ is an irreducible component of C, and f has d' irreducible factors.

Let us compute the finite sum $T_J = \sum_{j \in J} x_1\big(p_j(t)\big)$. The functions

$$u_j(t) = x_1(p_j(t)) \quad \text{and} \quad v_j(t) = x_2(p_j(t))$$

are holomorphic and satisfy for $j = 1 \ldots N$,

$$f(u_j(t), v_j(t)) = 0 \ , \quad q(u_j(t), v_j(t)) = t.$$

Differentiating this system, we deduce that

$$u_j{}'(t) = -\frac{\partial_{x_2} f}{\mathrm{Jac}(f,q)}(p_j(t)) \ , \ v_j{}'(t) = \frac{\partial_{x_1} f}{\mathrm{Jac}(f,q)}(p_j(t)).$$

Thus

$$T_J{}'(t) = -\sum_{j \in J} \frac{\partial_{x_2} f}{\mathrm{Jac}(f,q)}(p_j(t)).$$

The existence of the curve $C_J \subset C$ is then equivalent to $T_J{}'(t) = 0$ for q generic.

It remains to show the validity of step 4 in the algorithm. If C_J is a component of C, it has the same asymptotic behavior than C, i.e. the 0-cycle $C_t \cdot C_J$ converges to

$$D_Q \cdot C_J = k_3'(D_3 \cdot C_J) + \cdots + k_r'(D_r \cdot C_J).$$

The 0-cycle $C_t \cdot C_J = p_{j_1}(t) + \cdots + p_{j_{N'}}(t)$ is a sum of effective 0-cycles $Z_1(t), \ldots, Z_r(t)$, where $Z_i(t)$ has degree $k_i' \frac{l_i}{d'}$ and $Z_i(t) \to k_i' D_i \cdot C_J$. $\square$

5.1 Example

We apply our algorithm to the following simple (but not trivial) example:

$$\begin{aligned} f \quad = \quad & 49 + 30\,y\,x - 90\,y\,x^2 - 130\,x\,y^2 + 126\,y + 56\,x + 30\,x^2 - 3\,y^2 + x^4 + 8\,x^3 \\ & +36\,y^4 - 108\,y^3 - 127\,y^2\,x^2 + 32\,y^2\,x^3 - 54\,y\,x^3 + 84\,y^3\,x^2 + 37\,y^2\,x^4 \\ & -12\,y\,x^4 + 30\,y^3\,x^3 + 13\,x^2\,y^4 + 24\,x\,y^4. \end{aligned}$$

The Newton polytope P of f represented in Figure 3 is the convex hull of $\{(0,0), (4,0), (4,2), (2,4), (0,4)\}$.

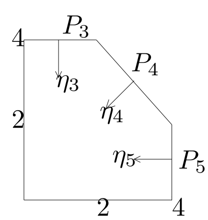

Figure 3:

The vectors $\eta_3 = (0,-1), \eta_4 = (-1,-1), \eta_5 = (-1,0)$, the integers $k_3 = 4, k_4 = 6, k_5 = 4, d = 2$, and Q is the convex hull of $\{(0,0), (2,0), (2,1), (1,2), (0,2)\}$. Let

$$q = -5 + 8x - 2y + x^2 + y^2 + 2xy^2 + 6yx^2.$$

Figure 4 helps the understanding of the principle of our algorithm on this example.

For $t = 10^3$, the intersection 0-cycle of the curve C_t defined by $q - t$ and the curve C defined by f is $C_t \cdot C = p_1 + \cdots + p_{14}$, with

$$
\begin{array}{rcl}
p_1 & = & (-3.788354357 - 22.18782564\, I,\ 0.1524031261 + 0.049759143\, I) \\
p_2 & = & (-3.788354357 + 22.18782564\, I,\ 0.1524031261 - 0.049759143\, I) \\
p_3 & = & (-2.389966107 - 4.663138871\, I,\ 7.365424369 + 1.227961352\, I) \\
p_4 & = & (-2.389966107 + 4.663138871\, I,\ 7.365424369 - 1.227961352\, I) \\
p_5 & = & (-1.986201832 - 22.37900395\, I,\ 0.1619217298 - 0.0018513709\, I) \\
p_6 & = & (-1.986201832 + 22.37900395\, I,\ 0.1619217298 + 0.0018513709\, I) \\
p_7 & = & (-1.535681765 - 1.726064601\, I,\ -9.102030424 + 7.399506679\, I) \\
p_8 & = & (-1.535681765 + 1.726064601\, I,\ -9.102030424 - 7.399506679\, I) \\
p_9 & = & (-1.045747272 - 3.489978116\, I,\ -5.189003901 + 9.662581013\, I) \\
p_{10} & = & (-1.045747272 + 3.489978116\, I,\ -5.189003901 - 9.662581013\, I) \\
p_{11} & = & (-0.7687604288 - 1.155834857\, I,\ 14.36735548 - 7.960507788\, I) \\
p_{12} & = & (-0.7687604288 + 1.155834857\, I,\ 14.36735548 + 7.960507788\, I) \\
p_{13} & = & (5.894022105 - 0.6210086653\, I,\ -6.648718394 + 5.938892046\, I) \\
p_{14} & = & (5.894022105 + 0.6210086653\, I,\ -6.648718394 - 5.938892046\, I).
\end{array}
$$

Now to determine $C \cdot D_i, i = 3, 4, 5$, we use toric affine coordinates (see Appendix) to find the three facet polynomials of f. Using the chart corresponding to the vertex $s_3 = (2, 4)$ with the coordinates $u = \frac{1}{x}, v = \frac{x}{y}$, we find

$$f_3(u) = 36u^2 + 24u + 13 \quad \text{and} \quad f_4(v) = 37v^2 + 30v + 12.$$

In the chart associated to $s_4 = (2, 4)$ with the coordinates $z = \frac{y}{x}, w = \frac{1}{y}$, we obtain $f_5(w) = w^2 - 12w + 37$. So we have

$$C \cdot D_3 = \{p_{3,1}, p_{3,2}\}\ ,\ C \cdot D_4 = \{p_{4,1}, p_{4,2}\}\ ,\ C \cdot D_5 = \{p_{5,1}, p_{5,2}\},$$

where

$$
\begin{array}{c}
u(p_{3,1}) = -\dfrac{1}{3} + \dfrac{1}{2}I\ ,\ v(p_{3,1}) = 0\ , \quad u(p_{3,2}) = -\dfrac{1}{3} - \dfrac{1}{2}I\ ,\ v(p_{3,2}) = 0\ , \\
v(p_{4,1}) = -\dfrac{15}{37} + \dfrac{16}{37}I\ ,\ u(p_{4,1}) = 0\ , \quad v(p_{4,2}) = -\dfrac{15}{37} - \dfrac{16}{37}I\ ,\ u(p_{4,2}) = 0\ , \\
w(p_{5,1}) = 6 + I\ ,\ z(p_{5,1}) = 0 \quad ,\ w(p_{5,2}) = 6 - I\ ,\ z(p_{5,2}) = 0,
\end{array}
$$

and

$$
\begin{array}{rcl}
f_3(u) & = & 36\big(u - u(p_{3,1})\big)\big(u - u(p_{3,2})\big), \\
f_4(v) & = & 37\big(v - v(p_{4,1})\big)\big(v - v(p_{4,2})\big), \\
f_5(w) & = & \big(w - w(p_{5,1})\big)\big(w - w(p_{5,2})\big).
\end{array}
$$

Now we collect the factors of f_i's to recover the factorization of f on the border $\Gamma = P_3 \cup P_4 \cup P_5$ of the Newton polytope P of f.

Since $C_t \cdot C = p_1(t) + \cdots + p_{14}(t)$, and $C_t \to 2D_3 + 3D_4 + 2D_5$, then 4 (resp. 6, and 4) points among these 14 converge to the 2 points in $C \cdot D_3$ (resp. $C \cdot D_4$, and $C \cdot D_5$), that is

$$p_1(t) + \cdots + p_{14}(t) \to 2(p_{3,1} + p_{3,2}) + 3(p_{4,1} + p_{4,2}) + 2(p_{5,1} + p_{5,2}).$$

More precisely, using the toric coordinates, we observe that the points p_1, p_6 (resp. p_3, p_{10}, p_{13}, and p_8, p_{12}) converge to $p_{5,1}$ (resp. $p_{4,1}$, and $p_{3,1}$). We deduce that

$$
\begin{array}{c}
J_{3,1} = \{8, 12\}\ \ ,\ \ J_{4,1} = \{3, 10, 13\}\ \ ,\ \ J_{5,1} = \{1, 6\}\ \ , \\
J_{3,2} = \{7, 11\}\ \ ,\ \ J_{4,2} = \{4, 9, 14\}\ \ ,\ \ J_{5,2} = \{13, 14\}.
\end{array}
$$

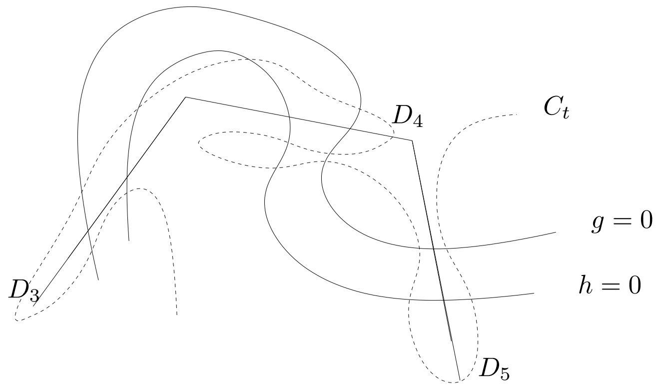

Figure 4:

Finally testing the vanishing of the expression (10), we find $\delta = 2, J_3 = \{1\}, J_4 = \{1\}, J_5 = \{1\}$. We deduce that the polynomial f admits 2 absolute irreducible factors g and h, and that the restriction of g on the 3 facets of P constituting Γ are (up to monomials)

$$g_3(u) = u - u(p_{3,1}), g_4(v) = v - v(p_{4,1}), g_5(w) = w - w(p_{5,1}).$$

We easily recognize that the extension $\mathbb{K} = \mathbb{Q}[I]$ with $I^2 = 1$. In this extension, the coefficients of polynomials are easily recognized from their decimal approximation.

Coming back to the toric coordinates (x, y), we find that the facet polynomials g_Γ (the restriction of g to Γ) and h_Γ are respectively

$$g_\Gamma = 6xy^2g_1 + xy^2g_3 = (2 - 3I)xy^2 + 6y^2 + (6 - I)x^2y - x^2,$$
$$h_\Gamma = (2 + 3I)xy^2 + 6y^2 + (6 + I)x^2y - x^2.$$

Remark 4 In this example to detect a partition of points defining the absolute factors of f we test $\binom{2}{1}\binom{2}{1}\binom{2}{1} = 6$ traces instead of $\binom{6}{3} = 20$ suggested by the original approach (see section 3, [20], [5]). In general using our approach based on the partition given in the step 4 of the algorithm, we have to test at most

$$\mathcal{N} = \sum_{\delta|n} \prod_{i=1}^{r} \binom{\frac{e_i}{\delta}}{e_i}$$

traces instead of the initial number

$$\mathcal{M} = \sum_{\delta|n} \binom{\frac{d}{\delta}}{d}.$$

Since $d = e_1 + \cdots + e_r$ and

$$\binom{a}{b}\binom{c}{d} < \binom{a+c}{b+d},$$

this shows that $\mathcal{N} < \mathcal{M}$, and the difference being increasing with the number of facets of the Newton polytope of f. Our algorithmic approach will bring efficiency in absolute factorization problem and improves subsequently the approach presented in [20, 5].

6 Conclusion

In this first paper, we established the mathematical bases of our algorithmic approach to toric factorization, and we verified that it works on some examples. However we still have to tune and improve the presented algorithm. This will be done in a future work together with improvements which will speed up it in many cases of interest. The method is symbolic-numeric and produces approximate absolute factors. To lift the approximate factorization to the exact one we can follow the approach in [20] and with some additional work, adapt [6].

Let us for instance notice that we could replace the polytope $Q = \frac{1}{d}N_f$ by a smaller one $\tilde{Q}$ having parallel facets. In particular in the bidegree case, we will take $\tilde{Q}$ equals to the unit square.

We will also investigate the possibility of cutting the curve C defined by f by special families of curves which will ease the computations.

Appendix on abstract toric surfaces

Let $Q \subset \mathbb{R}^2$ be a 2-dimensional integer convex polytope satisfying the condition of Lemma 1. Let us explain how to recover the embedded projective toric variety X_Q as an abstract algebraic one.

There exist unique primitive vectors[1] $\eta_1, \ldots, \eta_r$ in $\mathbb{Z}^2$ and unique positive integers $k_1, \ldots, k_r$ in $\mathbb{N}$, such that for $i = 1 \ldots r$, the facet Q_i of Q is included in the affine line

$$Q_i \subset \{m \in \mathbb{R}^2,\ \langle m, \eta_i \rangle + k_i = 0\},$$

where $\langle \cdot, \cdot \rangle$ is the usual scalar product in $\mathbb{R}^2$. The polytope Q is then given by the intersection of r affine half-planes:

$$Q = \{m \in \mathbb{R}^2 : \langle m, \eta_i \rangle + k_i \geq 0,\ \forall\, i = 1 \ldots r\}.$$

The vertices $s_1, \ldots, s_r$ of Q are in one-to-one correspondence with the facets of Q. If for $i = 1 \ldots r-1$, $s_i = Q_i \cap Q_{i+1}$, and $s_r = Q_r \cap Q_1$, any vertex s_i determines a 2-dimensional rational convex cone

$$\sigma_i := \{m \in \mathbb{R}^2 : \langle m, \eta_i \rangle \geq 0,\ \langle m, \eta_{i+1} \rangle \geq 0\}$$

dual to the cone $\eta_i \mathbb{R}^+ \oplus \eta_{i+1} \mathbb{R}^+$. Let

$$X_i := \mathrm{Spec}(\mathbb{C}[\sigma_i \cap \mathbb{Z}^2])$$

be the biggest variety on which all the Laurent polynomials supported in σ_i can be extended as regular functions. Such a variety is called an affine toric surface, since the torus $\mathbb{T} = (\mathbb{C}^*)^2$ is an open set of X_i and its action on itself extends to X_i.

We can glue naturally the affine surfaces X_i and X_{i+1}, corresponding to cones having a common 1-dimensional face, along their common set $X_i \cap X_{i+1}$ containing the torus $\mathbb{T}$. This natural gluing is compatible with the torus action and gives a complete normal variety X containing $\mathbb{T}$ as a Zariski open set. This

[1] A vector $v = (v_1, v_2) \in \mathbb{Z}^2$ is primitive if $\gcd(v_1, v_2) = 1$.

torus compactification is called the normal complete toric surface associated to Q. It can be written as

$$X = \mathbb{T} \cup D_1 \cdots \cup D_r,$$

where $D_1, \ldots, D_r$ are the unique irreducible divisors of X invariant under the torus action. Each D_i is isomorphic to $\mathbb{P}^1$ and meets the affine toric variety X_k if and only if $k \in \{i, i+1\}$.

For any $m \in \mathbb{Z}^2$, the Laurent monomial x^m is regular on the Zariski open set $\mathbb{T}$ common to all the charts X_i. It defines a rational function on X giving rise to a principal Cartier divisor $\mathrm{div}(x^m)$ supported on $X \setminus \mathbb{T}$, and equal to

$$\mathrm{div}(x^m) = \sum_{i=1}^{r} \langle m, \eta_i \rangle \, D_i.$$

More generally, any Laurent polynomial q gives rise to a principal Cartier divisor

$$\mathrm{div}(f) = C_f - b_1 D_1 - \cdots - b_r D_r,$$

where C_f is the Zariski closure in X of the effective divisor $\{f = 0\} \subset \mathbb{T}$, and

$$b_i = -\min\{\langle m, \eta_i \rangle, \ m \in N_f\} \ , \quad i = 1 \ldots r,$$

are integers, N_f is the Newton polytope of f. Conversely, to any toric divisor $D = \sum_{i=1}^{r} b_i D_i$, we can associate an integral polytope P_D

$$P_D = \{m \in \mathbb{R}^2 : \langle m, \eta_i \rangle + b_i \geq 0, \ i = 1 \ldots r\}$$

so that $\mathrm{div}(f) + D \geq 0$ if and only if the support of f is contained P_D, for any Laurent polynomial f. In other words, the set $H^0(X, \mathcal{O}_X(D))$ of global sections of the invertible sheaf corresponding to D is isomorphic to the set of Laurent polynomials supported by P_D, and admits the Laurent monomials $x^m, \ m \in P_D \cap \mathbb{Z}^2$, as a natural basis.

Let us denote by

$$D_Q = k_1 D_1 + \cdots + k_r D_r$$

the particular divisor associated to the given polytope Q (so that $Q = P_{D_Q}$). It is globally generated on X and gives rise to the Kodaira rational map

$$\phi_{D_Q} : X \longrightarrow \mathbb{P}(H^0(X, \mathcal{O}_X(D_Q)))^{\nu}$$

which sends a generic x on the point ζ_x corresponding to the hyperplane of global sections vanishing at x. If $x \in \mathbb{T}$, and $Q \cap \mathbb{Z}^2 = \{m_0, \ldots, m_l\}$, this hyperplane is

$$\{a = [a_0 : \cdots : a_l] \in \mathbb{P}(H^0(X, \mathcal{O}_X(D))) : \sum_{i=0}^{l} a_i x^{m_i} = 0\}.$$

So that the natural homogeneous coordinates of ζ_x for $x \in \mathbb{T}$ are

$$\phi_{D_Q}(x) = \zeta_x = [x^{m_0} : \cdots : x^{m_l}],$$

and ϕ_{D_Q} defines a morphism on the torus. The map ϕ_{D_Q} turns out to be an embedding precisely when $m_1 - m_0, \ldots, m_l - m_0$ generate the lattice $\mathbb{Z}^2$ (See

Lemma 1), in this case the toric variety X is isomorphic to the projective variety X_Q previously constructed. The divisor D_Q is then very ample and gives rise to the isomorphism

$$H^0(X, \mathcal{O}_X(D_Q)) = \phi_{D_Q}^* H^0(\mathbb{P}^l, \mathcal{O}_{\mathbb{P}^l}(1)) \simeq H^0(X_Q, (\mathcal{O}_{\mathbb{P}^l}(1))_{|X_Q}), \tag{11}$$

traducing that the closure in X of curves defined by generic Laurent polynomials supported by Q are isomorphic to some hyperplane sections of $X_Q \subset \mathbb{P}^l$. We notice that the genericity criterion is essential here: For example, if $f(x) = x^{m_i}$, then the curve defined by f is empty while the corresponding hyperplane section $X_Q \cap \{u_i = 0\}$ is not. Let us explicit this genericity criterion.

Lemma 3 *Assume that D_Q is very ample and let f be a reduced Laurent polynomial supported in dQ, $d \in \mathbb{N}^*$. Then $C_f \simeq X_Q \cdot H$, for a reduced hypersurface $H \subset \mathbb{P}^l$ of degree d if and only if the support of f meets every facets of dQ.*

Proof. The assumption $N_f \subset dQ$ is equivalent to $\mathrm{div}(f) = C_f - D_f$, where $D_f = b_1 D_1 + \cdots + b_r D_r$ is an effective divisor bounded by dD_Q. Thus $\mathrm{div}(f) = C_f + (dD_Q - D_f) - dD_Q$, and since $C_f + (dD_Q - D_f) \geq 0$, f defines a global section of $\mathcal{O}_X(dD_Q)$. We deduce from the isomorphism (11), the existence of an effective divisor H of degree d in $\mathbb{P}^l$ such that

$$C_f + (dD_Q - D_f) = H_{|X},$$

under the identification $X = X_Q$. Then $C_f = H_{|X}$ if and only if $dD_Q = D_f$, that is if the equality $b_i = dk_i$ holds for every $i = 1 \ldots r$. Moreover, as C_f is reduced, H must be reduced. □

References

[1] F. Abu Salem, S. Gao, and A. G. B. Lauder, *Factoring polynomials via polytopes*, in ISSAC 2004, ACM, New York, 2004, pp. 4–11.

[2] D. N. Bernstein, *The number of roots of a system of equations*, Funkcional. Anal. i Priložen., 9 (1975), pp. 1–4.

[3] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, in ISSAC 2004, ACM, New York, 2004, pp. 42–49.

[4] G. Chèze, *Absolute polynomial factorization in two variables and the knapsack problem*, in ISSAC 2004, ACM, New York, 2004, pp. 87–94.

[5] G. Chèze and A. Galligo, *Four lectures on polynomial absolute factorization*, in Solving polynomial equations, vol. 14 of Algorithms Comput. Math., Springer, Berlin, 2005, pp. 339–392.

[6] ———, *From an approximate to an exact absolute polynomial factorization*, J. Symbolic Comput., 41 (2006), pp. 682–696.

[7] G. Chèze and G. Lecerf, *Lifting and recombination techniques for absolute factorization*, J. Complexity, 23 (2007), pp. 380–420.

[8] D. A. Cox, *The homogeneous coordinate ring of a toric variety*, J. Algebraic Geom., 4 (1995), pp. 17–50.

[9] I. Z. Emiris, *On the complexity of sparse elimination*, J. Complexity, 12 (1996), pp. 134–166.

[10] W. Fulton, *Introduction to toric varieties*, vol. 131 of Annals of Mathematics Studies, Princeton University Press, Princeton, NJ, 1993. , The William H. Roever Lectures in Geometry.

[11] S. Gao, *Absolute irreducibility of polynomials via Newton polytopes*, J. Algebra, 237 (2001), pp. 501–520.

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

[13] I. M. Gel′fand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, Mathematics: Theory & Applications, Birkhäuser Boston Inc., Boston, MA, 1994.

[14] P. Griffiths and J. Harris, *Principles of algebraic geometry*, Wiley-Interscience [John Wiley & Sons], New York, 1978. Pure and Applied Mathematics.

[15] A. G. Hovanskiĭ, *Newton polyhedra and the Euler-Jacobi formula*, Uspekhi Mat. Nauk, 33 (1978), pp. 237–238.

[16] G. Lecerf, *Improved dense multivariate polynomial factorization algorithms*, J. Symbolic Comput., 42 (2007), pp. 477–494.

[17] I. Newton, *Curves*, Lexicon Technicum, 2 (1710).

[18] A. M. Ostrowski, *On multiplication and factorization of polynomials. I. Lexicographic orderings and extreme aggregates of terms*, Aequationes Math., 13 (1975), pp. 201–228.

[19] W. Ruppert, *Reduzibilität ebener Kurven*, J. Reine Angew. Math., 369 (1986), pp. 167–191.

[20] D. Rupprecht, *Semi-numerical absolute factorization of polynomials with integer coefficients*, J. Symbolic Comput., 37 (2004), pp. 557–574.

[21] T. Sasaki, M. Suzuki, M. Kolář, and M. Sasaki, *Approximate factorization of multivariate polynomials and absolute irreducibility testing*, Japan J. Indust. Appl. Math., 8 (1991), pp. 357–375.

[22] A. J. Sommese, J. Verschelde, and C. W. Wampler, *Numerical decomposition of the solution sets of polynomial systems into irreducible components*, SIAM J. Numer. Anal., 38 (2001), pp. 2022–2046 (electronic).

[23] ——, *Numerical factorization of multivariate complex polynomials*, Theoret. Comput. Sci., 315 (2004), pp. 651–669.

[24] J. von zur Gathen and E. Kaltofen, *Factoring sparse multivariate polynomials*, J. Comput. System Sci., 31 (1985), pp. 265–287. Special issue: Twenty-fourth annual symposium on the foundations of computer science (Tucson, Ariz., 1983).

[25] M. Weimann, *An interpolation theorem in toric varieties*, submitted (2007).

[26] J. A. Wood, *A simple criterion for local hypersurfaces to be algebraic*, Duke Math. J., 51 (1984), pp. 235–237.