Factoring bivariate polynomials using adjoints

Martin Weimann

Factoring bivariate polynomials using adjoints

Martin Weimann

Ricam, Austrian Academy of Sciences, Altenbergerstrasse 69, A-4040 Linz, Austria

Abstract

We relate factorization of bivariate polynomials to singularities of projective plane curves. We prove that adjoint polynomials of a polynomial $F \in k[x, y]$ with coefficients in a field k permit to recombinations of the factors of $F(0, y)$ induced by both the absolute and rational factorizations of F, and so without using Hensel lifting. We show in such a way that a fast computation of adjoint polynomials leads to a fast factorization. Our results establish the relations between the algorithms of Duval-Ragot based on locally constant functions and the algorithms of Lecerf and Chèze-Lecerf based on lifting and recombinations. The proof is based on cohomological sequences and residue theory.

Key words: Factorization, adjoint polynomials, curves, singularities, residues, cohomology.

1. Introduction

Factorization of multivariate polynomials is a central topic in Computer Algebra. We refer the reader to (Chèze, 2004; Chèze-Lecerf, 2007; Gathen-Gerhard, 2003) and to the references therein for recent surveys of the topic. In this article, we study the relations between singularities of projective plane curves and factorization of bivariate polynomials by using adjoint polynomials. In (Duval, 1991), an algorithm is given for absolute bivariate factorization based on locally constant rational functions on the curve, using normalization and rational Newton-Puiseux expansions. The best actual complexities for rational and absolute factorization have been obtained later on in (Lecerf, 2007) and (Chèze-Lecerf, 2007) by using the so-called method of lifting and recombination of modular factors. We establish here the bridge between these two approaches and we show that the factorization can be computed fast if we are given the adjoint polynomials.

Main result. Let $F \in k[x, y]$ be a bivariate polynomial defined over an arbitrary field k. We are interested in computing both the rational (over k) and absolute (over an algebraic

Email address: weimann23@gmail.com (Martin Weimann).
URL: http://people.ricam.oeaw.ac.at/m.weimann/ (Martin Weimann).

closure $\bar{k}$) factorizations of F. In all of the sequel (except Section 8), we assume that F satisfies the following hypothesis

$$\text{(H)} \qquad F(0,y) \text{ is separable of degree } d = deg(F).$$

In particular F is square-free. Let $\mathcal{C} \subset \mathbb{P}^2$ be the (reduced) projective curve over k defined by F. We say that $D \subset \mathbb{P}^2$ is an *adjoint curve* of $\mathcal{C}$ if it passes throw all singular points p of $\mathcal{C}$ (including infinitely near points) with multiplicity at least that of $\mathcal{C}$ minus one (see Section 4 for a more precise definition). We say that $H \in k[x,y]$ is an *adjoint polynomial* of F of degree n if it gives the dehomogenized equation of an adjoint curve of degree n. Adjoints may be computed by linear algebra from the resolution of singularities. We denote by

$$A \subset k[y]$$

the vector subspace spanned by the remainders modulo (x) of adjoint polynomials of F of degree $d-2$.

Our main result asserts that we can compute quickly both the rational and absolute factorizations of F from the knowledge of a basis of A. Let us be more precise. Suppose for a while that $k = \bar{k}$ to simplify. Our key result says that

$$\dim(A) = d - s,$$

where s is the number of irreducible factors of F. Moreover, let $F_1, \ldots, F_s$ be the irreducible factors of F. The classical *recombination problem* consists to find the factors of $F_j(0,y)$ for all j among the factors of $F(0,y)$. We show that given a basis for A, the recombination problem is reduced to solve a linear system over k of $d-s$ equations and d unknowns. In some sense, *A contains the minimal information for solving recombinations.* Once the recombination problem is solved, it remains to use a fast multifactor Hensel lifting to compute the F_j's (the situation is nevertheless more subtle when k is not assumed to be algebraically closed).

For our complexity analysis, we charge a constant cost for each arithmetic operation $(+,-,\times,\div)$ in the ground field and the equality test. We use the classical $\mathcal{O}$ notations for complexity, and we use $\tilde{\mathcal{O}}$ in order to hide logarithmic factors in cost estimates. We recall that two univariate polynomials over k of degree $\leq m$ can be multiplied with softly linear complexity $\widetilde{\mathcal{O}}(m)$ (Gathen-Gerhard, 2003, Thm 8.23). We denote by $2 \leq \omega < 3$ the matrix multiplication complexity exponent. We obtain the following complexity results:

Theorem 1. *Let k be a field with effective univariate factorization. There exists a deterministic algorithm that, given F satisfying (H) and given a basis of A, computes the rational factorization of F with one factorization in $k[y]$ of degree d plus*

$$\mathcal{O}(d^2(d-s)^{\omega-2}) \subset \mathcal{O}(d^\omega)$$

arithmetic operations over k, with s the number of irreducible rational factors of F.

Up to our knowledge, the actual best complexity for deterministic rational factorization of dense bivariate polynomials is $\mathcal{O}(d^{\omega+1})$ operations in k (Lecerf, 2007). Thus theorem 1 leads us to ask if we can compute efficiently a basis for A (see below for such a discussion).

The vector space A contains too enough information to compute the absolute factorization of F. By absolute factorization, we mean here the computation of a family of pairs of polynomials

$$\{(Q_1, q_1), \ldots, (Q_r, q_r)\}$$

where $q_i \in k[t]$ is monic, $Q_i \in k[x, y, t]$ and where

$$F(x, y) = \prod_{i=1}^{r} \prod_{q_i(\alpha)=0} Q_i(x, y, \alpha)$$

is the irreducible decomposition of F over $\bar{k}$. Note that such a representation is non unique. We obtain the following result:

Theorem 2. *Suppose that k has characteristic 0 or greater than $d(d-1)$. There exists a deterministic algorithm that, given F satisfying hypothesis (H) and given a basis of A, computes the absolute factorization of F within*

$$\widetilde{\mathcal{O}}(d^2(d-\bar{s})^{\omega-2} + \bar{s}d^3) \subset \widetilde{\mathcal{O}}(d^4)$$

arithmetic operations over k, with $\bar{s}$ the number of irreducible absolute factors.

We obtain in theorem 2 the same class of complexity $\widetilde{\mathcal{O}}(d^4)$ known for absolute deterministic factorization. Note that in contrast to the rational case, no univariate factorization is required here.

Following (Chèze-Lecerf, 2007), we obtain too a probabilistic algorithm. We use here the same probabilistic computational model in terms of computation trees as used in (Chèze-Lecerf, 2007). In particular, almost all the trees of a family are expected to be executable on a given input if the cardinality of k is infinite.

Theorem 3. *Suppose that k has characteristic 0 or greater than $d(d-1)$. Given F satisfying hypothesis (H) and given a basis of A, there exists a polynomial $S \in \bar{k}[t_1, \ldots, t_d]$ of degree at most $d(d-1)$ and a family of computation trees parametrized by $c \in k^d$ such that*

- *Any executable tree returns the absolute factorization of F;*
- *A tree is executable whenever $S(c) \neq 0$.*

The maximal cost of the trees is bounded by

$$\widetilde{\mathcal{O}}(d^2(d-\bar{s})^{\omega-2} + d^{\frac{\omega+3}{2}}) \subset \widetilde{\mathcal{O}}(d^{\frac{\omega+3}{2}})$$

arithmetic operations over k. If the cardinality of k is infinite, the algorithm returns the correct answer with probability one.

The complexity of theorem 3 has to be compared to the best known complexity $\widetilde{\mathcal{O}}(d^3)$ for absolute probabilistic factorization (Chèze-Lecerf, 2007).

Is such a method efficient? Up to our knowledge, the complexities obtained in the 3 previous theorems are all smaller or equal to the actual best complexities for factorization of dense bivariate polynomials. Of course, the input data A represents a very strong information, and our results lead immediately to the following question:

Is there an efficient way to compute a basis of A?

We obtain the following result, as a consequence of the Riemann-Roch theorem for reducible curves.

Theorem 4. *Given a basis of the vector space $Adj(d-2)$ of all adjoint polynomials of F of degree $d-2$, we compute a basis of A within*

$$\mathcal{O}(d^2(g+d-\bar{s})) \subset \mathcal{O}(d^4)$$

arithmetic operations over k, where g is the geometric genus of $\mathcal{C}$ (sum of the genus of the irreducible components).

The complexity of Theorem 4 is sharp: the k-vector space $Adj(d-2)$ of adjoint polynomials of degree $d-2$ has dimension $g+d-\bar{s}$ and the size of a basis of $Adj(d-2)$ is $\mathcal{O}(d^2(g+d-\bar{s}))$ field elements. So, computing a basis of A via first computing a basis for $Adj(d-2)$ and then reducing modulo x is not efficient, except maybe for deterministic absolute factorization (complexity $\widetilde{\mathcal{O}}(d^4)$) or for curves of small genus ($g \in \widetilde{\mathcal{O}}(d^{\omega-1})$ in order to stay in the class of complexity of deterministic rational factorization).

Suppose now that we are given an oracle that predicts a small genus (the extremal case being all irreducible components rational and $g=0$) and that we want to use Theorem 4 to compute a basis for A. Thus we need to compute a basis of $Adj(d-2)$. There are efficient algorithms for computing adjoints, by using Newton-Puiseux expansions (Stadelmeyer-Winkler, 1997) or integral basis (Mnũk, 1997; Deconinck-Van Hoeij, 2001), but whose complexities have not been analyzed yet. Unfortunately, even for small genus, it is still *a priori* hopeless that Theorem 4 gives an efficient method for computing A: one needs to know the normalization of the curve $\mathcal{C}$ for computing adjoints and we expect factorization to be a subprocedure of normalization. Up to our knowledge, if $k=\mathbb{F}_p$ with $p>d$, the best complexity for computing all singular Puiseux expansions of F is $\widetilde{\mathcal{O}}(d^5)$ operations (Poteaux-Rybowicz, 2011).

However, we will show (Section 9) that it's enough to separate all local branches $\mathcal{C}$ in order to compute A. In particular, we need not to desingularize irreducible branches. Moreover, we will see (Section 8) that in some cases, our method adapts too to the case $F(0,y)$ non separable, an important issue over fields of small caracteristic for which it might not exist a separable univariate specialization. In such a case, we can use some extra combinatorial information given by the resolution of singularities along the singular fiber to speed-up the algorithm. In that spirit, the author recently developed a factorization algorithm over $\mathbb{Q}[x,y]$ based on the toric resolution of the singularities at infinity (Weimann, 2010), running in polynomial time in the volume of the Newton polytope, improving (Lecerf, 2007) for sparse enough polynomials. A comparable result has recently been obtained in a different way in (Berthomieu-Lecerf, 2012), where the authors use a

clever deformation of the Newton polytope to bring back F to an almost dense polynomial. The algorithm in (Weimann, 2010) has an extra advantage to perform univariate factorizations of smaller degrees with a faster recombination, but it works only over number fields and assumes an extra hypothesis of separability of the facet polynomials.

To summarize, *unless someone can find a different way of computing A, we are unfortunately not going to get a better factorization algorithm using our approach.* Nevertheless, it's still not clear if the method developed here may be useful for some special type of polynomials (small degree components, smooth components, high singularities along a line, etc.), or if we are given some extra input data concerning the singularities (genus, discriminant, etc.). Anyway, despite of their hypothetical practical impacts, our results clarify the relations between normalization and factorization, giving a good point of view for comparing the classes of complexity of both operations and of various related algorithms (Newton-Puiseux, Hensel lifting, integral closure, etc.). It has to be noticed too that the hypothetic strength of our approach depends strongly on further improvements in the algorithmic theory of singularities, especially on the Newton-Puiseux algorithm.

Idea of the proof. Let us suppose that $k = \bar{k}$ to simplify. Let V be the vector space of meromorphic 1-forms of $\mathcal{C}$ that have only poles above $x = 0$. Each of these 1-forms gives an element of k^d given by its residues at the d places above $x = 0$. By the residue theorem, the sum of residues of a meromorphic form on a curve is zero. Thus, each form in V provides a linear relation between these residues, one relation for each irreducible component $\mathcal{C}_j$ of $\mathcal{C}$. Thus, with s irreducible components (factors), we get s independent linear relations for these d residues; this implies that the image of V in k^d by taking residues gives a subspace $W \subset k^d$ of dimension at most $d - s$. We will show that this subspace has exactly dimension $d-s$. The proof mainly uses the structural sheaf sequence of a divisor on the normalization of $\mathcal{C}$, combined with the Serre duality. Finally the theory of adjoints polynomials permits to show that V and W are respectively isomorphic to $Adj(d-2)$ and A. It follows that $\dim(A) = d - s$ so that *absolute recombinations and adjoints modulo (x) determine each other by solving a $d \times d$ linear system over k* (Corollary 18). Once the recombinations are solved, it remains to use a fast multifactor Hensel lifting to compute the factors. Roughly speaking, our method combines ideas developed in (Duval, 1991) and (Ragot, 1997) (computing locally constant rational functions) with ideas in (Lecerf, 2007) and (Chèze-Lecerf, 2007) (recombination of modular factors by Hensel lifting).

Organization. We introduce the recombination problem and its relation to locally constant functions in Section 2. In Section 3, we prove our key result that gives conditions for lifting locally constant functions using residue theory and cohomology. In Section 4, we establish the relation with adjoint polynomials and we prove Theorem 4. We solve recombinations in Section 5 from which follow the proofs of Theorem 1, 2 and 3 in Section 6. We illustrate our method and results on two simple examples in Section 7. In Section 8, we discuss the case $F(0, y)$ non separable with an illustrating example. In Section 9, we show that the computation of A does not require the all resolution of singularities and we conclude in the last Section 10.

Acknowledgements. We thank the referees and the editor for their helpful comments and suggestions. We thank especially the referee who pointed out a mistake in the computation of adjoints in the example of Section 8 and who gave us a Maple code for computing a basis of $Adj(d-2)$.

2. Recombinations and locally constant functions.

Our algorithms are related to (Lecerf, 2007) and (Chèze-Lecerf, 2007), both methods being based on the recombination problem of the modulo (x) factors. We first explain this problem and then we relate it to the sheaves of locally constant functions on the normalizing curve. We keep the same notations and hypothesis as in the introduction.

2.1. Recombinations problems

Let us consider the respective factorizations

$$\begin{cases} F(x,y) = F_1(x,y)\cdots F_s(x,y) \\ F(0,y) = f_1(y)\cdots f_n(y) \end{cases}$$

of F and F modulo (x) over k (recall that $F(0,y)$ is assumed to be separable). Solving *rational recombinations* consists in computing the vectors

$$\nu^{(j)} = (\nu_1^{(j)}, \ldots, \nu_n^{(j)}) \in \{0,1\}^n$$

induced by the relations

$$F_j(0,y) = \prod_{i=1}^{n} f_i(y)^{\nu_i^{(j)}}, \quad j = 1, \ldots, s.$$

In the same way, let

$$\begin{cases} F(x,y) = \bar{F}_1(x,y)\cdots \bar{F}_{\bar{s}}(x,y) \\ F(0,y) = \bar{f}_1(y)\cdots \bar{f}_d(y) \end{cases}$$

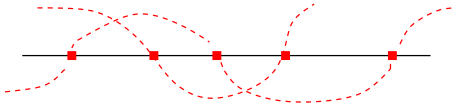
be the respective factorizations of F and F modulo (x) over $\bar{k}$. Solving *absolute recombinations* consists in computing the vectors

$$\bar{\nu}^{(j)} = (\bar{\nu}_1^{(j)}, \ldots, \bar{\nu}_d^{(j)}) \in \{0,1\}^d$$

induced by the relations

$$\bar{F}_j(0,y) = \prod_{i=1}^{d} \bar{f}_i(y)^{\bar{\nu}_i^{(j)}}, \quad j = 1, \ldots, \bar{s}.$$

The following picture illustrates the absolute recombinations when $\mathcal{C}$ is union of a cubic and a conic.



$$\Longrightarrow \qquad \bar{\nu}^{(1)} = (1,0,1,0,1), \quad \bar{\nu}^{(2)} = (0,1,0,1,0)$$

In this article we mainly pay attention to the recombination problems, the irreducible factorization of F then following with a fast multi-factor Hensel lifting (combined with a partial fraction decomposition algorithm in the absolute case). The main idea is to interpret the recombination problem as a cohomological problem of lifting sections.

2.2. *Solving recombinations* **via** *lifting sections*

All schemes and properties (connectivity, irreducibility) are considered over the base field k. We may think a point over a scheme X over a k as a collection of points in the extension $\bar{X} = X \otimes_k \bar{k}$ that are conjugated under the Galois group of $\bar{k}/k$.

Let $\mathcal{C}$ and $\mathcal{L}$ be the respective Zariski closures of the affine curves $F = 0$ and $x = 0$ to the projective plane $\mathbb{P}^2$. Let

$$\pi : X \to \mathbb{P}^2$$

be the weak embedded resolution of $\mathcal{C}$ (Kollár, 2007, Chap. 1.5, Thm 1.43) [1] . We denote by C and L the respective strict transforms of $\mathcal{C}$ and $\mathcal{L}$ by π. The inclusion of the zero-dimensional subscheme

$$Z := C \cap L$$

into C induces a restriction morphism

$$\alpha \, : \, H^0(\mathcal{O}_C) \hookrightarrow H^0(\mathcal{O}_Z)$$

between the respective k-vector spaces of regular functions on C and Z. Note that both vector spaces may be identified with the sets of locally constant functions on C and Z. The map α is injective since Z has at least one point on each component of C. The following two subsections are dedicated to show that the computation of the cokernel of α permits to solve both the rational and the absolute recombination problems.

2.2.1. *The rational case.*

Since $F(0, y)$ has degree d, Z is an affine zero-dimensional subscheme whose ring of regular functions may be identified with the finite k-algebra

$$H^0(\mathcal{O}_Z) = \frac{k[x, y]}{(x, F)} = \frac{k[y]}{(F(0, y))}. \tag{1}$$

Since $F(0, y)$ is separable, its rational factorization induces an isomorphism

$$H^0(\mathcal{O}_Z) \simeq \frac{k[y]}{(f_1)} \oplus \cdots \oplus \frac{k[y]}{(f_n)}. \tag{2}$$

Thus Z has n connected components (closed points) $p_1, \ldots, p_n$ corresponding to the maximal ideals of the ring $H^0(\mathcal{O}_Z)$ generated by the f_i's. The natural inclusions

$$k \hookrightarrow \frac{k[y]}{(f_i)}, \quad i = 1, \ldots, n$$

combined with (1) and (2) induce the inclusion

$$k^n \subset H^0(\mathcal{O}_Z),$$

k^n being identified with the subspace of locally constant functions on Z that take value in k, that is $(\nu_1, \ldots, \nu_n) \in k^n$ sends p_i to ν_i (in general, a function on Z takes values in the various residue fields $k[y]/(f_i)$). The map α introduced before is related to recombinations by the following lemma:

---

[1] In the mentionned theorem, the field is assumed to be perfect. Although computing desingularization over non perfect fields is much harder (Kollár, 2007, digression 1.49), the weak desingularization theorem remains true over non perfect fields (Kollár, 2007, Chap. 1.8).

Lemma 5. *The vector subspace $W \subset k^n$ defined by*

$$W := k^n \cap Im(\alpha)$$

admits $(\nu^{(1)}, \ldots, \nu^{(s)})$ as reduced echelon basis (up to reordering).

Proof. By definition, $\nu \in W$ if and only if it's the restriction to Z of a locally constant k-valued function on C. Since C is smooth, it has s connected components $C_1 \ldots, C_s$ corresponding to the prime rational factors of F. Thus $\nu \in W$ if and only if ν is k-valued and constant along $C_j \cap L$ for $j = 1, \ldots, s$. We deduce that $dim_k W = s$ and that $\nu^{(j)} \in W$ for $j = 1, \ldots, s$. Since the $\nu^{(j)}$'s have $\{0,1\}$-coordinates and are pairwise orthogonal vectors in k^n, they form up to reordering the reduced echelon basis of W. □

By Lemma 5, the recombination problem over k is reduced to compute first the rational factorization of $F(0, y)$ (inducing the inclusion $k^n \subset H^0(\mathcal{O}_Z)$), and then the cokernel of α.

2.2.2. The absolute case.

The relations between locally constant functions and absolute factorization is explored in (Duval, 1991) where the author determines one absolute factor a time from a basis of the regular functions on $C \times_k \bar{k}$. We rather relate here regular functions on C to the recombination algorithm in (Chèze-Lecerf, 2007) and we compute all irreducible factors simultaneously by using multi-factor Hensel lifting. Let us first prove:

Lemma 6. *We have equalities $dim_k H^0(\mathcal{O}_Z) = d$ and $dim_k H^0(\mathcal{O}_C) = \bar{s}$.*

Proof. First equality is clear from (1). Since $H^0(\mathcal{O}_C)$ is a finite dimensional k-vector space, we have

$$dim_k H^0(\mathcal{O}_C) = dim_{\bar{k}} H^0(\mathcal{O}_C) \otimes_k \bar{k}$$

Let $\bar{C} := C \times_k \bar{k}$ be the geometrical scheme associated to C by extending the base field k to its algebraic closure $\bar{k}$. We have (Liu, 2002, prop. 1.24 p.85)

$$H^0(\mathcal{O}_C) \otimes_k \bar{k} = H^0(\mathcal{O}_{\bar{C}}).$$

Since $\bar{C}$ is smooth, it's the *disjoint* union of $\bar{s}$ irreducible components $\bar{C}_1 \ldots, \bar{C}_{\bar{s}}$ corresponding in an obvious way to the prime absolute factors of F. It follows that we have an isomorphism of $\bar{k}$-vector spaces

$$H^0(\mathcal{O}_{\bar{C}}) \simeq \oplus_{j=1}^{\bar{s}} H^0(\mathcal{O}_{\bar{C}_j}).$$

Since $H^0(\mathcal{O}_{\bar{C}_j}) = \bar{k}$, we have $dim_{\bar{k}} H^0(\mathcal{O}_{\bar{C}}) = \bar{s}$ so that $dim_k H^0(\mathcal{O}_C) = \bar{s}$. □

Let $\phi_1, \ldots, \phi_d$ be the roots of $F(0, y)$ in $\bar{k}$. The identification (1) gives rise to the multi-evaluation isomorphism

$$\begin{array}{rccc} ev: & H^0(\mathcal{O}_Z) \otimes_k \bar{k} & \xrightarrow{\simeq} & \bar{k}^d \\ & \nu & \longmapsto & \bar{\nu} := (\nu(\phi_1), \ldots, \nu(\phi_d)). \end{array} \tag{3}$$

The next lemma shows that solving absolute recombinations reduces to compute $Im(\alpha)$ and to apply the evaluation map ev. We endow $\bar{k}^d$ with its canonical basis.

Lemma 7. *The vector subspace $\bar{W} \subset \bar{k}^d$ defined by*

$$\bar{W} := ev(Im(\alpha) \otimes_k \bar{k})$$

admits $(\bar{\nu}^{(1)}, \ldots, \bar{\nu}^{(\bar{s})})$ as reduced echelon basis (up to reordering).

Proof. Let $\bar{Z} := Z \times_k \bar{k}$. The map ev induces an identification

$$\bar{k}^d = H^0(\mathcal{O}_{\bar{Z}}),$$

where $\bar{\nu} = (\bar{\nu}_1, \ldots, \bar{\nu}_d) \in \bar{k}^d$ is identified with the locally constant function that sends each closed point $\bar{p}_i \in \bar{Z}$ to $\bar{\nu}_i$. Since $\bar{Z}$ contains at least one point of each connected component of $\bar{C}$, the restriction map

$$\bar{\alpha} \,:\, H^0(\mathcal{O}_{\bar{C}}) \hookrightarrow H^0(\mathcal{O}_{\bar{Z}})$$

is injective. By definition, $\bar{W} = Im(\bar{\alpha})$ so that $dim_{\bar{k}} \bar{W} = dim_{\bar{k}} H^0(\mathcal{O}_{\bar{C}}) = \bar{s}$ by the proof of Lemma 6. Each vector $\bar{\nu}^{(j)}$ being constant on $\bar{C}_1 \cap \bar{L}, \ldots, \bar{C}_{\bar{s}} \cap \bar{L}$, it extends to a function on $\bar{C}$. So $\bar{\nu}^{(j)} \in \bar{W}$ for $j = 1, \ldots, \bar{s}$. Since the $\bar{\nu}^{(j)}$'s have $\{0,1\}$-coordinates and are pairwise orthogonal in $\bar{k}^d$, they form up to reordering the reduced echelon basis of $\bar{W}$. □

3. Lifting sections using residues

The previous section shows that recombinations may be reduced to compute the cokernel of the restriction morphism

$$\alpha \,:\, H^0(\mathcal{O}_C) \hookrightarrow H^0(\mathcal{O}_Z).$$

To this aim, we introduce residues. We refer the reader to (Lipman, 2011; Serre, 1988; Tate, 1968; Vakil, 2008; Couvreur, 2009) for introductions of residues for curves and surfaces over arbitrary fields.

Let ω_C be the sheaf of regular differential 1-forms over C (the dualizing sheaf) and let $\omega_C(Z)$ be the sheaf of meromorphic 1-forms with polar divisor bounded by Z. Let $p \in C$ with residue field k_p and let $\psi \in \omega_{C,p}(Z)$ be a germ of meromorphic form at p. For any uniformizer t of C at p, there exists a unique formal series $h \in k_p[[t]]$ such that

$$\psi = \frac{h(t)dt}{t}.$$

We define *the residue of ψ at p* as

$$res_p \psi := Tr_p\,[h(0)],$$

where $Tr_p : k_p \to k$ is the trace map. This definition does not depend on the choice of the uniformizer (Serre, 1988). The map res_p is k-linear and vanishes on regular forms. In particular, if $\nu \in \mathcal{O}_{Z,p}$ has a local lifting $\widetilde{\nu}$ to $\mathcal{O}_{C,p}$, we check that the definition

$$\mathrm{res}_p(\nu\,\psi) := \mathrm{res}_p(\widetilde{\nu}\,\psi)$$

does not depend on the choice of the lifting. Moreover, we check too from the definition that for all $\psi \in \omega_{C,p}(Z)$ we have

$$\psi \in \omega_{C,p} \iff res_p(\nu\,\psi) = 0 \quad \forall\, \nu \in \mathcal{O}_{Z,p}, \tag{4}$$

which is the simplest realization of the local duality theorem (Lipman, 2011). We have the following key result:

Proposition 8. *There is an exact sequence of k-vector spaces*

$$0 \longrightarrow H^0(\mathcal{O}_C) \xrightarrow{\alpha} H^0(\mathcal{O}_Z) \xrightarrow{R} H^0(\omega_C(Z))^\vee \xrightarrow{\beta} H^0(\omega_C)^\vee \longrightarrow 0$$

where $^\vee$ stands for the dual and where R associates to ν the linear form

$$R_\nu : \ \psi \longmapsto \sum_{i=1}^{n} \mathrm{res}_{p_i}(\nu\psi).$$

In particular, $\dim H^0(\omega_C(Z)) = g + d - \bar{s}$ where g is the geometric genus of $\mathcal{C}$ (sum of the genus of the absolute irreducible components).

Proof. Let ω_Z be the dualizing sheaf of Z, so that $\omega_Z \simeq Hom(\mathcal{O}_Z, k)$. By (4), there is a short exact sequence (a particular realization of the so-called adjunction formula (Liu, 2002, Thm 9.1.39))

$$0 \longrightarrow \omega_C \longrightarrow \omega_C(Z) \xrightarrow{Res} \omega_Z \longrightarrow 0,$$

where the residue map Res is locally defined on an open set $U \subset C$ as

$$\begin{aligned} Res_U(\psi) : \mathcal{O}_Z(U) &\longrightarrow k \\ \nu &\longmapsto \sum_{p \in U} res_p(\nu\psi). \end{aligned}$$

The associated long exact cohomology sequence is

$$0 \to H^0(\omega_C) \to H^0(\omega_C(Z)) \xrightarrow{Res} H^0(\omega_Z) \to H^1(\omega_C) \to H^1(\omega_C(Z)). \tag{5}$$

By the duality of Serre (Liu, 2002, Rem. 6.4.20 and 7.3.27) , we get isomorphisms

$$H^1(\omega_C) \simeq H^0(\mathcal{O}_C)^\vee \quad \text{and} \quad H^1(\omega_C(Z)) \simeq H^0(\mathcal{O}_C(-Z))^\vee = 0,$$

the last vanishing property because Z as at least one point on each connected component of C. The dual sequence of (5) becomes

$$0 \to H^0(\mathcal{O}_C) \xrightarrow{\alpha} H^0(\mathcal{O}_Z) \xrightarrow{R} H^0(\omega_C(Z))^\vee \xrightarrow{\beta} H^0(\omega_C)^\vee \to 0$$

where R is dual to Res, that is

$$R : \nu \longmapsto \Big(\psi \mapsto \sum_{p_i \in Z} res_{p_i}(\nu\psi)\Big).$$

This shows the exact sequence of Proposition 8. This sequence induces equality

$$h^0(\omega_C(Z)) = h^0(\omega_C) + h^0(\mathcal{O}_Z) - h^0(\mathcal{O}_C) = g + d - \bar{s},$$

last equality using Lemma 6 and using that $h^0(\omega_C)$ coincides with the sum g of the geometric genus of the absolute irreducible components of $\mathcal{C}$. □

Remark 9. The inclusion $Im(\alpha) \subset ker(R)$ follows from the *residue theorem* that asserts that

$$\sum_{p \in C_j} res_p \psi = 0$$

for all connected component C_j of C and all rational 1-form ψ on C (Tate, 1968, Corollary of Thm 3).

Remark 10. The equality $dim\, H^0(\omega_C(Z)) = g+d-\bar{s}$ given by Proposition 8 follows from the *theorem of Riemann-Roch* for curves. This theorem is usually stated for irreducible curves over $\bar{k}$, but holds in the more general context of a not necessarily reduced or irreducible projective curve over a field k (Liu, 2002, Thm 7.3.26).

4. Relations with adjoint polynomials

We relate now holomorphic forms with adjoint polynomials. We denote by S the set of singular points of $\mathcal{C}$, including all infinitely near points. For each $p \in S$, there is a decomposition of π

$$X \xrightarrow{\pi_1} \widetilde{X}_p \xrightarrow{\pi_p} X_p \xrightarrow{\pi_2} \mathbb{P}^2$$

such that p is a closed point of the intermediary surface X_p and π_p is the blow-up at p (Kollár, 2007, Chap. 1.5). Let E_p be the exceptional divisor of π_p and $\hat{E}_p$ its total transform under π_1. We denote by m_p the multiplicity at p of the strict transform of $\mathcal{C}$ under the map π_2.

Definition 11. The *adjoint divisor* of F is the exceptional effective divisor

$$E := \sum_{p \in S} (m_p - 1)\hat{E}_p.$$

An *adjoint curve* of $\mathcal{C}$ is an effective divisor $D \subset \mathbb{P}^2$ that satisfies

$$\pi^*(D) \geq E.$$

An *adjoint polynomial* of F of degree $\leq m$ is a polynomial giving the dehomogeneised affine equation of an adjoint curve of degree m.

In other words, adjoints of F are those polynomials vanishing at the singular points of $\mathcal{C}$ with high enough multiplicities. Adjoints carry out precious informations about the geometry of $\mathcal{C}$. In particular, it is well known (Fulton, 2004, Chap. 3) that they are deeply related to the sheaf ω_C of regular forms on the normalized curve. Let us be more precise. We denote by

$$Adj(m) \subset k[x, y]$$

the k-vector subspace generated by adjoint polynomials of F of degree $\leq m$. We have the following proposition:

Proposition 12. *For all integers $m \leq 2$, we have an isomorphism*

$$\begin{aligned} Adj(d-3+m) &\xrightarrow{\simeq} H^0(\omega_C(mZ)) \\ H &\longmapsto \pi^*\Big(\frac{H dx}{x^m \partial_y F}\Big)_{|C}. \end{aligned}$$

Proof. In order to relate adjoints with differential forms, we introduce the *conductor*

$$\mathcal{A}_{\mathcal{C}} := Hom_{\mathcal{O}_{\mathcal{C}}}(\pi_* \mathcal{O}_C, \mathcal{O}_{\mathcal{C}})$$

of the normalization of $\mathcal{C}$. It is an ideal sheaf of $\mathcal{O}_{\mathcal{C}}$, related to the dualizing sheaf $\omega_{\mathcal{C}}$ of $\mathcal{C}$ by the formula

$$\pi_* \omega_C = \omega_{\mathcal{C}} \otimes_{\mathcal{O}_{\mathcal{C}}} \mathcal{A}_{\mathcal{C}}$$

(see for instance Szpiro, 1979, p.25). Since the morphism $\pi : C \to \mathcal{C}$ is affine we have

$$H^0(C, \omega_C(mZ)) = H^0(\mathcal{C}, \pi_*(\omega_C(mZ))) = H^0(\mathcal{C}, \omega_{\mathcal{C}}(m\mathcal{L}) \otimes \mathcal{A}_{\mathcal{C}}), \tag{6}$$

last equality following from the projection formula (recall that $Z = C \cap L$ and $\pi^* \mathcal{L} = L$). Let $\mathcal{A}$ be the inverse ideal sheaf of $\mathcal{A}_{\mathcal{C}}$ under the restriction $\mathcal{O}_{\mathbb{P}^2} \to \mathcal{O}_{\mathcal{C}}$. We have the short exact sequence

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}^2}(-\mathcal{C}) \longrightarrow \mathcal{A} \longrightarrow \mathcal{A}_{\mathcal{C}} \longrightarrow 0. \tag{7}$$

Tensoring (7) with the invertible sheaf $\Omega^2_{\mathbb{P}^2}(\mathcal{C} + m\mathcal{L})$, and using the adjunction formula (Liu, 2002, Thm 9.1.37), we obtain the exact sequence

$$0 \longrightarrow \Omega^2_{\mathbb{P}^2}(m\mathcal{L}) \longrightarrow \Omega^2_{\mathbb{P}^2}(\mathcal{C} + m\mathcal{L}) \otimes \mathcal{A} \xrightarrow{RP} \omega_{\mathcal{C}}(m\mathcal{L}) \otimes \mathcal{A}_{\mathcal{C}} \longrightarrow 0. \tag{8}$$

Here, RP is the Poincaré residue map [2], defined outside the singular locus of $\mathcal{C}$ as

$$RP\Big(\frac{H dx \wedge dy}{F x^m}\Big) = \Big(\frac{H dx}{x^m \partial_y F}\Big)_{|\mathcal{C}}. \tag{9}$$

For $m \leq 2$ and $i = 0, 1$, we have (Hartshorne, 1977, Theorem 5.1 p.225)

$$H^i(\mathbb{P}^2, \Omega^2_{\mathbb{P}^2}(m\mathcal{L})) = H^i(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(m-3)) = 0$$

which, combined with the long exact cohomological sequence of (8), gives an isomorphism

$$RP : H^0(\mathbb{P}^2, \Omega^2_{\mathbb{P}^2}(\mathcal{C} + m\mathcal{L}) \otimes \mathcal{A}) \xrightarrow{\simeq} H^0(\mathcal{C}, \omega_{\mathcal{C}}(m\mathcal{L}) \otimes \mathcal{A}_{\mathcal{C}}). \tag{10}$$

By (Szpiro, 1979, Proposition p.33), we have an isomorphism [3]

[2] The Poincaré residue is originally defined for complex manifolds, and is rather called 1-codimensional residues over arbitrary fields (Couvreur, 2009).

[3] We check that the irreducibility assumption made in (Szpiro, 1979, Proposition p.33) can be removed since the proof is local.

$$\begin{aligned} Adj(d-3+m) &\xrightarrow{\simeq} H^0(\mathbb{P}^2, \Omega^2_{\mathbb{P}^2}(\mathcal{C}+m\mathcal{L}) \otimes \mathcal{A}) \\ H &\longmapsto \frac{H dx \wedge dy}{F x^m} \end{aligned}$$

which combined with (6), (9) and (10) gives the isomorphism of Proposition 12. □

Remark 13. The isomorphism of Proposition 12 for $m = 0$ and $\mathcal{C}$ irreducible is known as the Gorenstein Theorem (Gorenstein, 1952) which asserts that the adjoint curves of degree $d-3$ cut out on $\mathcal{C}$ the complete canonical system of its normalization. For a nice down-to-earth presentation of adjoints and conductors, see (Fulton, 2004).

Recall from the introduction that we define $A \subset k[y]$ to be the image of the projection

$$\begin{aligned} Adj(d-2) &\longrightarrow k[y] \\ H &\longmapsto H(0,y). \end{aligned}$$

Corollary 14. *We have equality* $dim_k\, A = d - \bar{s}$.

Proof. If $H \in Adj(d-2)$ satisfies $H(0,y) \equiv 0$, then $H(x,y) = xH'(x,y)$ for some polynomial H'. Since the line $x = 0$ does not contain any singularities of $\mathcal{C}$, H' is necessarily an adjoint of F of degree $d-3$. In other words, we have an exact sequence of k-vector spaces

$$0 \longrightarrow Adj(d-3) \longrightarrow Adj(d-2) \longrightarrow A \longrightarrow 0 \tag{11}$$

where the first map is the injective "multiplication by x" map and the second map is the restriction to $x = 0$. It follows that

$$\begin{aligned} \dim(A) &= \dim Adj(d-2) - \dim Adj(d-3) \\ &= h^0(\omega_C(Z)) - h^0(\omega_C) \\ &= d - \bar{s}, \end{aligned}$$

second equality using Proposition 12 and last equality using Proposition 8. □

The proof of Theorem 4 follows.

Corollary 15. *(Proof of Theorem 4). Given a basis of* $Adj(d-2)$*, we can compute a basis of* A *within*

$$\mathcal{O}(d^2(g+d-\bar{s})) \subset \mathcal{O}(d^4)$$

arithmetic operations over k.

Proof. Consider the matrix N whose set of rows is a basis of $Adj(d-2)$ evaluated at $x = 0$, expressed in the natural basis of $k[y]$. The complexity for building N is esesentially the size of $Adj(d-2)$, that is $\mathcal{O}(d^2(g+d-\bar{s}))$ arithmetic operations. The matrix N has $d-1$ columns and $g+d-\bar{s}$ rows (use Propositions 8 and 12). By (11), we have $A = Im(N)$, and

a basis of A can be computed within the expected complexity $\mathcal{O}((d-1)(g+d-\bar{s})(d-\bar{s})^{\omega-2})$ (Storjohann, 2000, Theorem 2.10). We conclude with the well known inequalities $g \leq (d-1)(d-2)/2$ and $2 < \omega \leq 3$. $\square$

5. Recombinations follow

We have now all necessary information for solving recombinations. Let us consider first the rational case.

Corollary 16. *We have an exact sequence of k-vector spaces*

$$0 \longrightarrow \langle \nu^{(1)}, \ldots, \nu^{(s)} \rangle \longrightarrow k^n \xrightarrow{T} A^\vee$$

where T sends $\nu = (\nu_1, \ldots, \nu_n)$ to the linear map

$$H \longmapsto \sum_{i=1}^{n} \nu_i \left(\sum_{f_i(\phi)=0} \frac{H(\phi)}{\partial_y F(0,\phi)} \right).$$

Proof. By Lemma 5, we have

$$\langle \nu^{(1)}, \ldots, \nu^{(s)} \rangle = Im(\alpha) \cap k^n$$

where we identify $k^n \subset H^0(\mathcal{O}_Z)$ with the subspace of locally constant k-valued functions on Z. Proposition 8 induces equality

$$Im(\alpha) \cap k^n = \Big\{ \nu \in k^n, \quad \sum_{i=1}^{n} \nu_i res_{p_i}(\psi) = 0 \quad \forall\ \psi \in H^0(\omega_C(Z)) \Big\}.$$

Let us compute the involved residues. By Proposition 12, $\psi \in H^0(\omega_C(Z))$ is equal to

$$\psi = \pi^* \Big(\frac{H dx}{\partial_y F x} \Big)_{|C}$$

for a unique $H \in Adj(d-2)$. Let $\widehat{\mathcal{O}}_{C,p_i}$ be the completion of the regular local ring $\mathcal{O}_{C,p_i}$ with respect to its maximal ideal associated to p_i. The residue field of C at p_i is equal to

$$k_{p_i} = \frac{k[y]}{(f_i)}.$$

The map π being an isomorphism in a neighborhood of p_i, we have an isomorphism

$$\begin{aligned} \widehat{\mathcal{O}}_{C,p_i} &\xrightarrow{\simeq} k_{p_i}[[t]] \\ \pi^* x &\longmapsto t \\ \pi^* y &\longmapsto a(t) \end{aligned}$$

where $a \in k_{p_i}[[t]]$ is the unique series such that $a(0)$ is the residue class of y in k_{p_i} and $F(t, a(t)) \equiv 0$. In such a local system of coordinates, ψ is equal to

$$\psi = \frac{H(t, a(t))}{\partial_y F(t, a(t))} \frac{dt}{t}$$

and it follows from the definition of residues that

$$res_{p_i}(\psi) = Tr_{p_i}\Big(\frac{H(0,a(0))}{\partial_y F(0,a(0))}\Big) = \sum_{f_i(\phi)=0}\Big(\frac{H(0,\phi)}{\partial_y F(0,\phi)}\Big).$$

Corollary 16 follows. □

Remark 17. We always have $(1,\dots,1) \in ker(T)$. This is nothing else than the Lagrange interpolation formula.

Let us now consider the absolute case.

Corollary 18. *We have an exact sequence of $\bar{k}$-vector spaces*

$$0 \longrightarrow \langle \bar{\nu}^{(1)},\dots,\bar{\nu}^{(\bar{s})}\rangle \longrightarrow \bar{k}^d \xrightarrow{\bar{T}} A^\vee \otimes_k \bar{k} \longrightarrow 0$$

where $\bar{T}$ sends $\bar{\nu} = (\bar{\nu}_1,\dots,\bar{\nu}_d)$ to the linear form

$$H \longmapsto \sum_{i=1}^{d} \bar{\nu}_i \frac{H(\phi_i)}{\partial_y F(0,\phi_i)}.$$

Proof. Apply Proposition 8 and repeat the proof of Corollary 16 over $\bar{k}$, with the curve $\bar{C}$ replacing C. Surjectivity of $\bar{T}$ follows from Corollary 14. □

Remark 19. In (Chèze-Lecerf, 2007; Lecerf, 2007), the authors solve recombinations using a system of $\mathcal{O}(d^2)$ equations. Corollary 16 and Corollary 18 give a much smaller number $d-\bar{s}$ of equations for recombinations. Moreover, the map $\bar{T}$ being surjective, $d-\bar{s}$ is the expected minimal number of linear conditions for recombinations in the absolute case.

6. Proofs of Theorems 1, 2 and 3.

We can now prove the three main theorems exposed in the introduction.

6.1. Proof of Theorem 1.

We suppose here that the field k supports univariate factorization. We obtain the following algorithm.

Algorithm 1 **(deterministic rational factorization)**

Input: $F \in k[x,y]$ that satisfies hypothesis (H).
Output: The rational factorization of F.

- Step 1. Compute a basis of A.

- Step 2. If $\dim A = d-1$, F is irreducible. Otherwise, compute the irreducible factors $f_1, \ldots, f_n$ of $F(0,y)$ over k.
- Step 3. If $n = 1$, F is irreducible. Otherwise, build the matrix M of the map T of Corollary 16 by using Newton identities.
- Step 4. Compute the reduced echelon normal basis of $ker(M)$. We obtain the recombination vectors $\nu^{(1)}, \ldots, \nu^{(s)}$.
- Step 5. Compute the factorization of $F(0,y)$ induced by the recombination vectors and lift it to the rational factorization of F.

Proposition 20. *(Proof of Theorem 1.) Algorithm* 1 *is deterministic and correct. Steps* 3, 4 *and* 5 *take at most*

$$\mathcal{O}(n(d-\bar{s})(d-s)^{\omega-2} + d^2) \subset \mathcal{O}(d^\omega)$$

arithmetic operations over k.

Proof. The algorithm is deterministic and correct thanks to Corollary 16. Let us describe in more details the content and the complexity of steps 3 to 5.

Step 3. In order to build the matrix M, we have to compute

$$Tr_{k_{p_i}}\Big(\frac{H(y)}{\partial_y F(0,y)}\Big)$$

for all $i = 1, \ldots, n$ and for all H running a basis of A. Inversion of $\partial_y F(0,y)$ and multiplication by H in $k[y]/(f_i)$ take $\mathcal{O}(n_i)$ operations in k. Then $H/\partial_y F(0,y) \in k[y]/(f_i)$ is uniquely represented as a polynomial $a(y) = a_0 + \cdots + a_{n_i-1}y^{n_i-1}$ with coefficients in k and

$$Tr_{k_{p_i}}\Big(\frac{H(y)}{\partial_y F(0,y)}\Big) = \sum_{j=0}^{n_i-1} a_j Tr_{k_{p_i}}(y^j). \tag{12}$$

Thanks to the Newton identities, we can compute recursively the trace of y^j from the traces of smaller powers of y and from the coefficients of f_i with j multiplications and j additions. So we compute traces of all involved powers of y within $\mathcal{O}(n_i^2)$ operations over k. Given these traces, and using (12), we compute the trace of $H/\partial_y F$ with $2n_i$ operations for each $H \in A$. By Corollary 14, it follows that step 3 costs $\sum_{i=1}^{n} \mathcal{O}(n_i^2 + 2n_i(d-\bar{s})) \subset \mathcal{O}(d^2)$ operations over k.

Step 4. The matrix M has size $(d-\bar{s}) \times n$ and rank $d-s$. We can compute the reduced echelon normal basis of the kernel of M within $\mathcal{O}(n(d-\bar{s})(d-s)^{\omega-2})$ operations ((Storjohann, 2000), Theorem 2.10).

Step 5. Given a vector $\nu^{(j)} = (\nu_i^{(j)}) \in \{0,1\}^n$ of the reduced echelon basis, we compute $F_j(0,y) = \prod f_i(y)^{\nu_i^{(j)}}$ for each rational irreducible factor F_j of F. This requires $\widetilde{\mathcal{O}}(deg(F_j(0,y)))$ operations by the sub-product tree technique (Lecerf, 2007, proof of Prop. 6), so a total cost of $\widetilde{\mathcal{O}}(d)$ operations. To compute the F_j's, it's now enough to lift the induced equality $F(0,y) = F_1(0,y)\cdots F_s(0,y)$ modulo (x) up to precision modulo (x^{d+1}). This costs $\widetilde{\mathcal{O}}(d^2)$ operations by using Newton quadratic iteration (Gathen-Gerhard, 2003, Theorem 15.18). □

6.2. Proofs of Theorems 2 and 3

In the absolute case, the delicate point is that Corollary 18 does not permit to solve recombinations with linear algebra over k. Moreover, it neither permits to describe the smallest finite extensions over which the irreducible absolute factors of F are defined. To solve this problem, we rather rely our approach with the algorithms 8 and 9 in (Chèze-Lecerf, 2007), where the authors use the absolute partial fraction decomposition algorithm of Lazard-Rioboo-Trager (Lazard-Rioboo, 1990).

Let ϕ be the residue class of y in the ring $\mathbb{A} := k[y]/(F(0,y))$. Any element $b \in \mathbb{A}$ can be uniquely represented as a finite sum

$$b = \sum_{i=0}^{d-1} b_i \phi^i$$

where $\mathrm{coeff}(b, \phi^i) := b_i$ belongs to k. We introduce

$$L := \Big\{ v \in k^d, \quad \sum_{i=1}^{d} v_i \,\mathrm{coeff}\Big(\frac{H(\phi)}{\partial_y F(0,\phi)}, \phi^{i-1}\Big) = 0 \quad \forall\ H \in A \Big\}.$$

The vector space L is related to the absolute recombinations by the following lemma.

Lemma 21. *Let V be the Vandermonde matrix of the roots $\phi_1, \ldots, \phi_d$ of $F(0,y)$. We have an isomorphism*

$$V^t : \langle \bar{\nu}^{(1)}, \ldots, \bar{\nu}^{(\bar{s})} \rangle \xrightarrow{\simeq} L \otimes_k \bar{k}.$$

In particular, we have an isomorphism of k-vector spaces

$$B : Im(\alpha) \xrightarrow{\simeq} L$$

where $B = (Tr\phi^{i+j})_{i,j=0,\ldots,d-1}$, with $Tr : \mathbb{A} \to k$ the usual trace map.

Proof. We follow the proof of Proposition 4 in (Chèze-Lecerf, 2007). Let $(v_1, \ldots, v_d) = V^t(w_1, \ldots, w_d)$ and let $b \in \mathbb{A}$. We have

$$\begin{aligned} \sum_{i=1}^{d} v_i \,\mathrm{coeff}(b, \phi^{i-1}) &= \sum_{i=1}^{d} \big(\sum_{j=1}^{d} w_j \phi_j^i \big) \,\mathrm{coeff}(b, \phi^{i-1}) \\ &= \sum_{j=1}^{d} w_j \big(\sum_{i=1}^{d} \mathrm{coeff}(b, \phi^{i-1}) \phi_j^i \big) = \sum_{j=1}^{d} w_j b(\phi_j). \end{aligned}$$

The first point then follows from Corollary 18 by taking $b = H(\phi)/\partial_y F(0,\phi)$. The second point follows from Lemma 7 since V is the matrix of the evaluation map and $B = V^t V$ is the matrix of traces. □

We can now rely on the factorization algorithms developed by Chèze-Lecerf in the absolute case. We refer the reader to (Chèze-Lecerf, 2007) for details on the relations between absolute recombinations, absolute partial fraction decomposition, absolute Hensel lifting and absolute factorization.

Algorithm 2 (deterministic absolute factorization).

Input: $F \in k[x,y]$ that satisfies hypothesis (H), with k a field of characteristic 0 or greater than $d(d-1)$.

Output: The absolute factorization of F.

- Step 1. Compute a basis of A. If $\dim A = d-1$, F is absolutely irreducible.
- Step 2. Compute a basis of L.
- Step 3. Call Algorithm 8 in (Chèze-Lecerf, 2007) with input F and the basis of L.

Proposition 22. *(Proof of Theorem 2.) Algorithm 2 is deterministic and correct. Steps 2 and 3 take at most*

$$\widetilde{\mathcal{O}}(d(d-\bar{s})^{\omega-1} + \bar{s}d^3) \subset \widetilde{\mathcal{O}}(d^4)$$

arithmetic operations over k.

Proof. The algorithm is correct thanks to Lemma 21 combined with Proposition 4 p.15 and Theorem 5 p.15 in (Chèze-Lecerf, 2007). By definition, we have $L = ker(N)$, where the matrix N is built from a basis of A using one inversion in A and $(d-\bar{s})$ multiplications in $\mathbb{A}$, so $\mathcal{O}(d(d-\bar{s}))$ operations over k. Then, computing a basis of $L = ker(N)$ requires $\mathcal{O}(d(d-\bar{s})^{\omega-1})$ operations over k. Finally, step 3 costs $\widetilde{\mathcal{O}}(\bar{s}d^3)$ operations over k thanks to Proposition 10 p.24 in (Chèze-Lecerf, 2007). □

The cost of Algorithm 2 is dominated by the separation of residues in Algorithm 8 of (Chèze-Lecerf, 2007) that ensures that the call to the Lazard-Rioboo-Trager algorithm returns a correct answer. If we rather deal with a random linear combination of the vectors of a basis of L, we obtain a probabilistic algorithm with smaller complexity.

Algorithm 3 (probabilistic absolute factorization).

Input: $F \in k[x,y]$ that satisfies hypothesis (H), with k a field of characteristic 0 or greater than $d(d-1)$.

Output: The absolute factorization of F.

- Step 1. Compute a basis of A. If $\dim A = d-1$, F is absolutely irreducible.
- Step 2. Compute a basis of L.
- Step 3. Choose $c \in k^{\bar{s}}$, where $\bar{s} = d - dim(A)$.
- Step 4. Call Algorithm 9 in (Chèze-Lecerf, 2007) with input F, the basis of L and c.

Proposition 23. *(Proof of Theorem 3.) Algorithm 3 either stops prematurely or return a correct answer. Moreover, there exists a polynomial $S \in \bar{k}[C_1, \ldots, C_{\bar{s}}]$ of degree at most $\bar{s}(\bar{s}-1)$ such that the answer is correct whenever $S(c) \neq 0$. In any cases, steps 2, 3 and 4 take at most*

$$\widetilde{\mathcal{O}}(d(d-\bar{s})^{\omega-1} + d^{\frac{\omega+3}{2}})$$

arithmetic operations over k.

Proof. The proof is the same as for Proposition 22, using now Proposition 11 p.25 in (Chèze-Lecerf, 2007). □

Remark 24. The restriction hypothesis on the characteristic of k ensures the possibility to separate the residues and to apply a fast absolute multi-factor Hensel lifting in (Chèze-Lecerf, 2007, Algorithm 9).

7. Two simple examples

Let us illustrate our main results on two simple examples of small degrees.

Example 1. Suppose we want to compute the rational and absolute factorization of

$$F = y^5 + 3y^4 + x^2y^3 + 2y^3 - 2x^3y^2 + 3x^2y^2 - y^2 + 3x^2y - 3y - 2x^5 + 2x^3 + 2x^2 - 2$$

over $\mathbb{Q}$. The univariate polynomial $f(y) := F(0, y)$ factorizes over $\mathbb{Q}$ as

$$f = (y-1)\,(y+1)\,(y+2)\left(y^2+y+1\right),$$

and we have 4 modular factors to recombine. The projective curve $\mathcal{C}$ of F is a degree 5 curve with 6 nodes that all lie in the affine plane, solutions of the algebraic system

$$S = \{F = \partial_x F = \partial_y F = 0\}.$$

We find here that the $\mathbb{Q}$-vector space $Adj(d-2) = Adj(3)$ of degree 3 polynomials vanishing at these 6 points has dimension

$$\dim\, Adj(3) = \frac{(3+1)(3+2)}{2} - 6 = 4,$$

with basis

$$\big(y^3 + 2y^2 + 3y - 2x^3 - x^2 + 3\,,\, 3y^2 - x^2y + 4y + 2x^3 + 2\,,$$
$$y^3 + 2xy^2 + 3y^2 + 3y - 2x + 2\,,\, y^3 + 4y^2 + 3y - 2x^3 + x^2 + 1\big).$$

Taking reduction modulo (x), we find that A has dimension 3 with $\mathbb{Q}$-basis

$$A = \langle y^3 + 2y^2 + 3y + 3, 3y^2 + 4y + 2, y^3 + 4y^2 + 3y + 1\rangle.$$

We deduce from Corollary 14 that F admits

$$\bar{s} = d - \dim\, A = 2$$

irreducible absolute factors, hence $s \in \{1, 2\}$ irreducible factors over $\mathbb{Q}$.

To find the factors over $\mathbb{Q}$, we need to construct the matrix M of the map T of Proposition 25. Let $H \in A$. For $f_1 = y - 1$ the first factor of f, we have equality

$$Tr_{f_1}\Big(\frac{H}{f'}\Big) = \frac{H(1)}{f'(1)}.$$

For $f_2 = y + 1$ and $f_3 = y + 2$, we find in the same way

$$Tr_{f_2}\Big(\frac{H}{f'}\Big) = \frac{H(-1)}{f'(-1)} \quad \text{and} \quad Tr_{f_3}\Big(\frac{H}{f'}\Big) = \frac{H(-2)}{f'(-2)}.$$

For $f_4 = y^2 + y + 1$, we find

$$Tr_{f_4}\Big(\frac{H}{f'}\Big) = Tr_{f_4}(h)$$

where h is the reduction of H/f' modulo (f_4). Since f_4 has degree 2, h has degree 1 and by linearity, it's enough to compute $Tr_{f_4}(y^i)$ for $i = 0, 1$. We have here

$$Tr_{f_4}(1) = 2 \qquad \text{and} \qquad Tr_{f_4}(y) = -1.$$

We deduce in that way that the 3×4 matrix of the map T in Proposition 25 is

$$M = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{2} & \frac{1}{2} & -\frac{2}{3} & \frac{2}{3} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{3} & -\frac{1}{3} \end{pmatrix}$$

We find that

$$\ker(M) = \langle (1, 1, 0, 0), (0, 0, 1, 1) \rangle$$

so that F has $s = 2$ irreducible factors F_1 and F_2 over $\mathbb{Q}$ thanks to Proposition 25. Moreover, the modular factors recombine as

$$F_1(0, y) = f_1 f_2 = y^2 - 1 \qquad \text{and} \qquad F_2(0, y) = f_3 f_4 = y^3 + 3y^2 + 3y + 2.$$

Using a multifactor Hensel lifting up to precision (x^6) (it's enough to take $6 = d + 1$), we obtain finally $F = F_1 F_2$ where

$$F_1 = y^2 + x^2 - 1 \quad \text{and} \quad F_2 = y^3 - 2x^3 + 3y^2 + 3y + 2.$$

Since we already know that $\bar{s} = 2$, it follows that $F = F_1 F_2$ represents too the absolute irreducible factorization of F. Note that the projective curves with affine equations $F_1 = 0$ and $F_2 = 0$ have respective genus 0 and 1. Thus the total geometric genus of the curve $\mathcal{C}$ of F is $g = 1$, according to the formula

$$\dim\, Adj(d-2) = 4 = g + d - \bar{s}$$

predicted by Proposition 8 and Proposition 12.

Example 2. Let $k = \mathbb{Q}$. Suppose that we want to compute the rational and absolute factorization of

$$F(x, y) = y^4 - 2xy^2 - 4x^3y + 8x^2y - 4xy - x^4 + 6x^3 - 11x^2 + 8x - 2$$

We find here that $F(0, y) = y^4 - 2$ is irreducible over $\mathbb{Q}$ so that F is irreducible over $\mathbb{Q}$ too. Let us look at its absolute factorization. We find that the projective curve $\mathcal{C}$ of F has 4 singular points over $\bar{\mathbb{Q}}$

$$\Big((\frac{1 - \sqrt{3}\, i}{2}, 1), (\frac{\sqrt{3}\, i + 1}{2}, 1), (\frac{1}{2}, -\frac{1}{2}), (1, 0) \Big)$$

and we find that $\dim_{\mathbb{Q}}\, Adj(2) = 2$, with basis

$$Adj(2) = \langle y^2 - xy + x - 1, 2y^2 - xy + x^2 - 1 \rangle_{\mathbb{Q}}.$$

Taking reduction modulo (x), we find that $\dim_{\mathbb{Q}}\, A = 2$, with basis

$$A = \langle y^2 - 1, 2y^2 - 1 \rangle_{\mathbb{Q}}.$$

By Corollary 14, it follows that F admits exactly

$$\bar{s} = d - \dim\ A = 2.$$

irreducible absolute factors. To get these factors, there remains to compute a basis of the 2-dimensional vector space L introduced in Subsection 6.2. To this aim we compute the residue classes of $H(y)/\partial_y F(0,y)$ modulo (y^4-2) for H running over a basis of A. We find that

$$\frac{y^2-1}{4y^3} \equiv \frac{y^3-y}{8} \mod (y^4-2) \quad \text{and} \quad \frac{2y^2-1}{4y^3} \equiv \frac{2y^3-y}{8} \mod (y^4-2)$$

so that

$$L = \ker \begin{pmatrix} 0 & -\frac{1}{8} & 0 & \frac{1}{8} \\ 0 & -\frac{1}{8} & 0 & \frac{1}{4} \end{pmatrix} = \langle (1,0,0,0), (0,0,1,0) \rangle.$$

Then we call Algorithm 8 in (Chèze-Lecerf, 2007) with input F and the basis of L. We find the two absolute irreducible factors

$$F = \left(y^2 - t\,x\,y - t\,x^2 + x^2 + 2\,t\,x - x - t\right)\ \left(y^2 + t\,x\,y + t\,x^2 + x^2 - 2\,t\,x - x + t\right),$$

where t is the residue class of y in $\mathbb{Q}[y]/(y^2-2)$.

8. The case $F(0,y)$ non separable

When $F(0,y)$ is not separable modulo (x), we are tempted to choose another fiber $x = a$ for which $F(a,y)$ that satisfies hypothesis (H). There are two main reasons to develop a recombination algorithm along a critical fiber. First, when the field k has small positive characteristic, a regular fiber may not exist. Second, we show here that working along a singular fiber may in fact be an opportunity to speed-up the algorithm.

In order to simplify, we suppose here that $k = \bar{k}$. We suppose too that $F(0,y)$ has degree d (the general case follows easily by computing residues at $y = \infty$).

Our results generalise well to the non separable case, the main difference being related to the computation of residues. Let $Z = C \cap L$ where $L = \pi^*(\mathcal{L})$. In contrast to the previous sections, L and Z need not to be reduced anymore. The support of Z consists now in $r \leq d$ closed points $p_1, \ldots, p_r$ in one-to-one correspondance with the irreducible analytic branches of $\mathcal{C}$ along the line $\mathcal{L}$. The recombination vectors may now be defined in the smaller ambient space k^r, where $\mu^{(j)} \in k^r$ is defined to have ith coordinate equal to 1 if $p_i \in C_j$ and equal to 0 otherwise. By identifying k^r with the vector subspace of $H^0(\mathcal{O}_Z)$ of locally constant functions on Z with values in k *and with zero nilpotent part*, we obtain the analoguous of Lemma 5

$$\langle \nu^{(1)}, \ldots, \nu^{(s)} \rangle = Im(\alpha) \cap k^r, \tag{13}$$

where $\alpha : H^0(\mathcal{O}_C) \to H^0(\mathcal{O}_Z)$ still stands for the restriction map. We obtain the following generalization of Corollary 16:

Proposition 25. *We have an exact sequence of k-vector spaces*

$$0 \longrightarrow \langle \nu^{(1)}, \dots, \nu^{(s)} \rangle \longrightarrow k^r \xrightarrow{T} A^\vee$$

where T sends $\nu = (\nu_1, \dots, \nu_r)$ to the linear map

$$H \longmapsto \sum_{i=1}^{r} \nu_i \, res_{p_i}\Big(\pi^*\Big(\frac{H(y)dy}{F(0,y)}\Big)\Big).$$

Proof. The exact sequence of Proposition 8 remains valid in this new context. Combined with (13), we obtain that $\langle \nu^{(1)}, \dots, \nu^{(s)} \rangle = ker\, \widetilde{T}$ where $\widetilde{T} : k^r \to H^0(\omega_C(Z))^\vee$ sends $\nu = (\nu_1, \dots, \nu_r)$ to the linear map

$$\psi \longmapsto \sum_{i=1}^{r} \nu_i res_{p_i}(\psi).$$

The main difference concerns the computation of residues. Let $\psi \in H^0(\omega_C(Z))$. By the proof of Proposition 12, we have

$$\psi = RP_C(\Psi), \qquad \Psi = \pi^*\left(\frac{H(x,y)dx \wedge dy}{xF(x,y)}\right) \in H^0(\Omega^2_X(C+L))$$

for a unique $H \in Adj(d-2)$, and where RP_C stands for the Poincaré residue along C. Let $p \in C \cap L$. By (Couvreur, 2009, Theorem 6.3 and Remark 6.9), we obtain equality

$$res_p(\psi) = res_p\Big(RP_C(\Psi)\Big) = res_p\Big(RP_L(\Psi)\Big).$$

where the last residue stands for residue of 1-form on L. Since $L = \pi^*(\mathcal{L})$ and the Poincaré residue commutes with the pull-back, we obtain equality

$$RP_L\left(\pi^*\left(\frac{H(x,y)dx \wedge dy}{xF(x,y)}\right)\right) = \pi^*\left(RP_{\mathcal{L}}\left(\frac{H(x,y)dx \wedge dy}{xF(x,y)}\right)\right) = \pi^*\left(\frac{H(0,y)dy}{F(0,y)}\right).$$

Proposition 25 follows. □

So as soon as the curve $\mathcal{C}$ has a small number of irreducible branches intersecting $\mathcal{L}$, Proposition 25 permits to solve the recombination problem in a smaller ambient space. The price to pay is that we can *a priori* not compute residues directly in $\mathbb{P}^2$ as in Section 2, but we may really need to compute residues in X, using local coordinates or Puiseux series. Nevertheless, in the important case of $\mathcal{C}$ locally irreducible at $(0, y_p) \in \mathcal{C} \cap \mathcal{L}$, there is exactly one point $p \in C$ such that $\pi(p) = (0, y_p)$ and the residue can be computed directly in $\mathbb{P}^2$:

$$res_p\left(\pi^*\Big(\frac{H(y)dy}{F(0,y)}\Big)\right) = res_{y_p}\Big(\frac{H(y)dy}{F(0,y)}\Big).$$

Of course y_p may be now be a multiple root of $F(0,y)$ so the residue computation may involve higher order derivatives of H and F.

Example. *Let us illustrate Proposition 25 on a simple example. Suppose that we want to factorize*

$$F(x,y) = y^5 + y^4 - xy^3 - y^3 - 2xy^2 - y^2 + x^2 + xy + x.$$

over $\mathbb{Q}$. *The irreducible factorization of* F *mod* (x) *is*

$$F(0,y) = y^2(y+1)^2(y-1),$$

with two double roots -1 *and* 0 *and one simple root* 1. *Since* $\partial_x F(0,-1)$ *and* $\partial_x F(0,0)$ *do not vanish, the curve* $\mathcal{C}$ *is smooth and tangent to* $\mathcal{L}$ *at these two points, and transversal to* $\mathcal{L}$ *at* $(0,1)$. *In particular,* $\mathcal{C}$ *has only* 3 *irreducible branches intersecting* $\mathcal{L}$ *at distinct points and the recombinations will hold in the ambient space* k^3 *rather than in the bigger space* k^5 *inherent to a choice of a regular fiber.*

We have here

$$Adj(d-2) = \langle y^3 - y - 1, y^2 - x, , y^3 - xy\rangle$$

from which it follows that

$$A = \langle y+1, y^2, y^3\rangle.$$

By Lemma 6, the curve $\mathcal{C}$ *has* $deg(F) - dim(A) = 2$ *absolute irreducible components. Let* $H \in A$. *Since* F *is locally irreducible at* $(0,0)$, *we have equality*

$$res_0\Big(\frac{H(y)dy}{F(0,y)}\Big) = res_0\Big(\frac{H(y)dy}{y^2(y+1)^2(y-1)}\Big) = H'(0) + H(0).$$

In the same way, a simple calculation gives

$$res_{-1}\Big(\frac{H(y)dy}{F(0,y)}\Big) = \frac{-2H'(-1) - 5H(-1)}{4} \qquad \text{and} \qquad res_1\Big(\frac{H(y)dy}{F(0,y)}\Big) = \frac{H(1)}{4}.$$

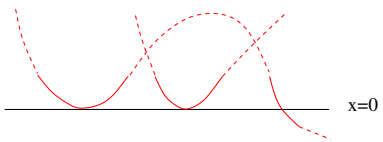
We deducesthat the 3×3 *matrix of the map* T *in Proposition 25 is*

$$M = \begin{pmatrix} -1/2 & -1/4 & -1/4 \\ 0 & 0 & 0 \\ 1/2 & 1/4 & 1/4 \end{pmatrix}$$

so that $ker(M) = ((0,1,0),(1,0,1))$. *We deduce the irreducible rational decomposition*

$$\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$$

where $\mathcal{C}_1$ *is a conic tangent to* $\mathcal{L}$ *at* $(0,0)$ *and* $\mathcal{C}_2$ *is a (smooth) cubic tangent to* $\mathcal{L}$ *at* $(0,1)$ *and transversal to* $\mathcal{L}$ *at* $(0,-1)$.



Since the induced factors of F are coprime modulo (x), we can compute them use a multifactor Hensel lifting (Gathen-Gerhard, 2003, Algorithm 15.17) up to a sufficiently high precision (mod (x^3) in our case). We obtain finally

$$F(x,y) = (y^2 - x)((y+1)^2(y-1) - x).$$

In summarize, we have shown here that working along a critical fiber may be an opportunity to speed-up the algorithm, at least when F satisfies the weaker hypothesis

(H′) $\mathcal{C}$ is analytically irreducible at each point of $\mathcal{C} \cap \mathcal{L}$.

First, the univariate factorization of $F(0,y)$ is faster since it is reduced to a fast separable factorization (Lecerf, 2008) plus some univariate factorizations of smaller degrees. Second, recombinations are faster since they hold in a smaller ambient space of dimension the number of distinct roots of $F(0,y)$ (or irreducible factors in the rational case). This fact is well illustrated in a previous work of the author (Weimann, 2010) who developed a lifting and recombination algorithm based on the toric resolution of the singularities of $\mathcal{C}$ along the line at infinity.

Remark 26. We can show that under hypothesis (H'), building the matrix of the map T has the same cost in the separable and non separable cases. The fact that the computations of the residues may involve f_i-adic expansions with higher precision for each irreducible factors f_i of $F(0,y)$ is compensed by the fact that the sum of the degrees of the f_i's decreases.

Remark 27. Although Proposition 25 still permit to solve recombinations even when F does not satisfy (H'), the problem resides in the fact that the irreducible factors of F may not be coprime modulo (x) and can not be computed with Hensel's lemma. This problem will be explored in a further work.

9. Don't touch the cusps

It turns out that the computation of A does not necessarily require to compute the all resolution of singularities of $\mathcal{C}$. Namely, let us consider the factorization of π

$$X \longrightarrow X_0 \xrightarrow{\pi_0} \mathbb{P}^2$$

where π_0 is the minimal composition of blow-ups under which the strict transform C_0 of $\mathcal{C}$ is every where locally irreducible. Then we can check that all our results (Lemmas 5, 6, 7 and the key Proposition 12) remain valid with C_0 replacing C and with the arithmetic genus $p_a(C_0) \geq g$ of C_0 replacing the geometric genus of $\mathcal{C}$ (the proofs mainly only use that the irreducible and connected components of C coincide). Then, we check easily that there is an exact sequence

$$0 \longrightarrow Adj_0(d-3) \xrightarrow{\times x} Adj_0(d-2) \xrightarrow{x=0} A \longrightarrow 0$$

where $Adj_0(k)$ is defined similarly as $Adj(k)$ with the map π_0 replacing π in Definition 11. For instance, we need not to desingularize cusps for computing A, which is of course natural from our factorization point of view. Note that there are easy local irreducibility sufficient criterions that can be directly read off from the Newton polygon of the singularity (for cusps for instance).

10. Conclusion

We have established the bridge between locally constant functions (Duval, 1991; Ragot, 1997) and lifting and recombinations algorithms (Lecerf, 2007; Chèze-Lecerf, 2007). We have shown that the vector space A of adjoint polynomials modulo (x) allows to recombine modular factors without using Hensel lifting and with the expected number of linear equations. Unfortunately, computing A using all adjoint polynomials uses too strongly the geometry of singularities and *a priori* doesn't lead a better factorization algorithm. So the question is:

"Is there an efficient way to compute a basis for A?"

Maybe such a way exists for some particular polynomials, for instance if the irreducible components are smooth and intersect in few points.

Finally, we discussed the possibility of speed-up the algorithm when $F(0, y)$ is not separable, an approach that hasn't been fully explored yet. Our general feeling is that it may be promising to develop some intermediary algorithms based on the resolution of only some of the singularities, in the vein of (Weimann, 2010) that uses the toric resolution of the singularities at infinity. In any cases, the power of using singularities for factorization depends strongly on complexity issues in the algorithmic theory of singularities, especially on the Newton-Puiseux algorithm.

References

K. Belabas, M. Van Hoeij, J. Klüners, A. Steel, *Factoring polynomials over global fields*, J. of Symb. Comp. Vol. 40, no 6 (2005), pp. 1325-1339.

J. Berthomieu, G. Lecerf, *Reduction of bivariate polynomials from convex-dense to dense, with application to factorizations*, Math. Comp. 81, no 279 (2012), pp.1799-1821.

E. Brieskorn, H. Knörrer, *Plane algebraic curves*, Birkhuser Basel (1986).

G. Chèze, *Des méthodes symboliques-numériques et exactes pour la factorisation absolue des polynômes en deux variables*, PhD thesis, http://www.math.univ-toulouse.fr/ cheze/mespublis.html.

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

A. Couvreur, *Sums of residues on algebraic surfaces and applications to coding theory*, J. of Pure and Applied Algebra 213 (2009), pp. 2201-2223.

B. Deconinck, M. Van Hoeij, *Computing Riemann matrices of algebraic curves*, PhysicaD, 152 (2001), pp. 28-46.

D. Duval, *Absolute factorization of polynomials, a geometric approach*, SIAM J. Comput. 20, No. 1 (1991), pp. 1-21.

W. Fulton, *Adjoints and Max Noether's Fundamentalsatz*, Algebra, arithmetic and geometry with applications, Springer (2004), pp. 301-313.

J. von zur Gathen, J. Gerhard, *Modern computer algebra*, second ed., Cambridge University Press, Cambridge, MA, (2003).
D. Gorenstein, *An arithmetic theory of adjoint plane curves*, Trans. Amer. Math. Soc. 72, (1952), pp.414-436.
R. Hartshorne, *Algebraic geometry*, Sringer-Verlag (1977).
R. Hartshorne, *Residues and Duality*, Lecture Notes in Math. 20, Springer-Verlag, (1989).
J. Kollár, *Lectures on resolution of singularities*, Ann. Math. Studies 166, (2007).
D. Lazard, R. Rioboo, *Integration of rational functions: rational computation of the logarithmic part*, J. Symbolic Comput., 9 (1990), pp.113-115.
G. Lecerf, *New recombination algorithms for bivariate polynomial factorization based on Hensel lifting*, Applicable Algebra in Engineering, Communication and Computing 21, no 2 (2010), pp 151-176.
G. Lecerf, *Fast separable factorization and applications*, Applicable Algebra in Engineering, Communication and Computing 19, no.2 (2008).
J. Lipman, *Residues, Duality, Fundamental Class*, Notes for Algecom 4, Purdue (2011).
Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics, 6 (2002).
M. Mnũk, *An Algebraic Approach to Computing Adjoint Curves*, J. Symbolic Computation 23 (1997), pp.229-240
A. Poteaux, M. Rybowicz *Complexity Bounds for the rational Newton-Puiseux Algorithm over Finite Fields*, Appl. Alg. in Eng., Comm. and Comp. 22, no 3 (2011), pp. 187-217.
J.-F. Ragot, *Sur la factorisation absolue des polynômes*, PhD thesis, Université de Limoges, France (1997).
J.-P. Serre, *Algebraic Groups and class fields*, Graduate texts in Mathematics, 117, Springer-Verlag, New York, (1988).
L. Szpiro, *Lectures on equations defining space curves*, Notes by N. Mohan Kumar, Tata Institute of Fundamental Research, Bombay, Springer-Verlag (1979).
P. Stadelmeyer, F. Winkler, *Computing the System of Adjoint Plane Curves by Puiseux Expansion*, Tech. report 97-38 RISC Report Series, Univ. Linz, Austria (1997).
A. Storjohann, *Algorithms for matrix canonical forms*, PhD thesis, ETH, Zürich, Switzerland (2000).
J. Tate, *Residues of differentials on curves*, Annales scientifiques de l'E.N.S. 4e série, tome 1, no 1 (1968), pp. 149-159.
R. Vakil, *An algebraic proof of Riemann-Roch*, manuscript, available at math.stanford.edu/ vakil/725/bagsrr.pdf.
M. Van Hoeij, *An algorithm for computing an integral basis in an algebraic function field.*, J. Symb. Comput., 18 (1994), pp. 353-363.
C.T.C Wall, *Singular points of plane curves*, London Math. Society (2004).
M. Weimann, *Algebraic osculation and factorization of sparse polynomials*, arXiv 0904.0178v1, to appear in J. of Found. of Comp. Math.
M. Weimann, *A lifting and recombination algorithm for rational factorization of sparse polynomials*, J. of Complexity, Vol. 26, no 6 (2010), pp. 608-628.