Bivariate Factorization Using a Critical Fiber

Martin Weimann

Bivariate factorization using a critical fiber

Martin Weimann

LMNO, Université de Caen BP 5186, F 14032 Caen Cedex

Abstract

We generalize the classical lifting and recombination scheme for rational and absolute factorization of bivariate polynomials to the case of a critical fiber. We explore different strategies for recombinations of the analytic factors, depending on the complexity of the ramification. We show that working along a critical fiber leads in some cases to a good theoretical complexity, due to the smaller number of analytic factors to recombine. We pay a particular attention to the case of polynomials that are non degenerate with respect to their P-adic Newton polytopes.

Key words: Bivariate polynomial, Factorization, Residues, Resultant, Valuation, Newton polytope, Algorithm, Complexity.

1. Introduction

Factorization of bivariate polynomials is a central topic of Computer Algebra for which many algorithms have been proposed, see for instance the surveys [17, 18] and the detailed introduction in [9]. Maybe the most successful method is the lifting and recombination scheme: given $F \in \mathbb{K}[x, y]$ a bivariate polynomial of bi-degree (d_x, d_y) over a field $\mathbb{K}$, and assuming separability with respect to y, we compute the factors of F in $\mathbb{K}[[x]][y]$ with a suitable precision and we recombine these analytic factors to recover the polynomial factors of F. Up to our knowledge, this approach led to the best theoretical complexity for factoring dense bivariate polynomials, see [24, 26, 5]. However, it has only been developed in the case when the fiber $x = 0$ is regular, that is when $F(0, y)$ is separable of degree d_y. In this article, we generalize it to the case of a critical (non regular) fiber, both for rational and absolute factorization issues. A first motivation for this work is that for fields with few elements, a regular fiber might not exist. Although working in a well chosen field extension can solve this problem [15], this might have a significant practical overhead [3]. A second motivation is that a critical fiber brings new combinatorial constraints that might speed up the recombination process. In particular, the number of absolute analytic factors to recombine necessarily decreases along a critical fiber, due do the

Email address: weimann@unicaen.fr (Martin Weimann).

presence of ramification. Our main result is the existence of a deterministic algorithm that, given the analytic factors of F up to a certain precision m, returns the rational factors of F in small polynomial time in the total degree. While the regular case requires a precision $m = d_x + 1$ [26], polynomials with high x-valuation of the discriminant might need a higher precision for solving recombinations with linear algebra. However, we show that in positive characteristic, the precision $d_x + 1$ is always enough to compute the numbers of rational factors and that in zero characteristic the precision $2d_x$ is enough to test irreducibility. Moreover, we exhibit different combinatorial tricks that allow to solve recombinations with precision $d_x + 1$ in many reasonable situations (Subsection 4.4). The algorithms we develop here are not intended to compete in general with actual implementations, but we illustrate on some examples that working along a critical fiber improves the complexity at least in some particular cases, especially for polynomials that are non degenerate or locally irreducible along the fiber. The strength of our results depends strongly on the complexity of analytic factorization, an issue we have not studied here.

Main result. The prime divisors of F in the rings $\mathbb{K}[[x]][y]$ and $\mathbb{K}[x, y]$ are respectively called analytic and rational factors. The n-truncated analytic factorization of F is the data of the residues modulo x^{n+1} of the irreducible analytic factors of F. Although it is a fundamental step of our algorithm, we do not pay attention here to the analytic factorization and we introduce the notation $\mathcal{C}(n, d_y)$ for the number of arithmetic operations over $\mathbb{K}$ required for computing the n-truncated analytic factorization of a polynomial $F \in \mathbb{K}[x, y]$ of degree d_y in y. When $x = 0$ is a regular fiber, it's well known that $\mathcal{C}(n, d_y) \subset \widetilde{\mathcal{O}}(nd_y)$ thanks to the multi-factor Hensel lifting [16]. We use here the classical $\widetilde{\mathcal{O}}$ notation in order to hide logarithmic factors in cost estimates [16, Ch. 25.7]. In general, analytic factorization is more tricky and $\mathcal{C}(n, d_y)$ is expected to be closely related to the complexity of Puiseux series computation.

Our main hypothesis on F is the following:

(H) *F is separable with respect to y.*

We can always reduce to hypothesis (H) after applying a separable factorization algorithm. For fields with at least $d_x(2d_y + 1)$ elements, the cost of computing separable factorization is $\widetilde{\mathcal{O}}(d_x d_y^2)$ by Proposition 8 in [25]. This is negligible when compared to all complexity results we obtain here. Hence, hypothesis (H) might be restrictive for us only for fields with few elements.

We denote by:

- p the characteristic of $\mathbb{K}$.
- s the number of irreducible analytic factors of F in $\mathbb{K}(x)[y]$. We thus have $s \leq d_y$.
- $q = \lfloor v/d \rfloor$ the integer part of the quotient of the x-adic valuation v of the y-discriminant of F with the minimal degree d of the analytic factors. This complexity indicator q will be refined in terms of the resultants and the discriminants of the analytic factors (see Section 3).
- ω the universal matrix multiplication exponent: multiplication of two $n \times n$ matrices costs $\mathcal{O}(n^\omega)$ operations in the base ring. It's well known that $2 \leq \omega \leq 2.5$ [16].

We refer the reader to Gathen and Gerhard's book [16] for elementary algorithms with polynomials (we recall the complexity of the main basic operations in Section 6). In all of the sequel, we assume that fast multiplication of polynomials is used. Hence two polynomials in $\mathbb{K}[y]$ of degrees at most d can be multiplied in softly linear time $\widetilde{\mathcal{O}}(d)$ [16, Theorem 8.23].

Theorem 1. *Let $m := \max(q, d_x+1)$. There exists a deterministic algorithm that, given $F \in \mathbb{K}[x,y]$ satisfying hypothesis (H), returns its irreducible rational factorization with at most*

- *$\mathcal{O}(md_y s^{\omega-1}) + \mathcal{C}(m, d_y)$ arithmetic operations over $\mathbb{K}$ if $p = 0$ or $p > d_x(2d_y-1)$;*
- *$\mathcal{O}(kmd_y s^{\omega-1}) + \mathcal{O}(k)\mathcal{C}(m, d_y)$ arithmetic operations over $\mathbb{F}_p$ if $\mathbb{K} = \mathbb{F}_{p^k}$.*

We have $q \in \mathcal{O}(d_x d_y)$ under hypothesis (H) and q can reach this order of magnitude (Section 3, Example 2.2). If the fiber is regular, then $q = 0$ in which case our algorithm specializes to that of Lecerf [26], with a complexity $\mathcal{O}(d_x d_y^\omega)$. For fields with at least $2d_y - 3$ elements, we can always find a fiber over which $q \leq d_x + 1$, see Remark 3.7. Over such a fiber, we get a complexity $\mathcal{O}(d_x d_y^\omega) + \mathcal{C}(d_x, d_y)$. The only difference with Lecerf's algorithm is that we need to compute the truncated analytic factorization along a critical fiber, a difficulty that is compensated by an expected smaller number s of analytic factors to recombine. It's an open question to know if $\mathcal{C}(d_x, d_y) \subset \mathcal{O}(d_x d_y^\omega)$. An important case is that of *non degenerate* polynomials, for which all edge polynomials of $F(x, y-\alpha)$ have simple roots for all $\alpha \in \mathbb{P}^1_{\bar{\mathbb{K}}}$. In that case, $q \leq d_x$ and s is strictly smaller to the total number of lattice points of all edges (see Section 8 for details). In such a case, the analytic factorization reduces after some well chosen monomial change of variables to the classical Hensel lifting or Newton iteration strategies. A brute force complexity analysis leads in that case to $\mathcal{C}(d_x, d_y) \subset \mathcal{O}(s d_x d_y^2)$ but we strongly believe that this result is not optimal.

Example. Suppose given two co-prime positive numbers a and b and a field $\mathbb{K}$ of characteristic zero or greater or equal to $2a+b$. Let

$$F(x,y) = (y^a + x^b + y^a x^b)(x^a y^b + 1)((y-1)^a + x^b + x^b(y-1)^a) \in \mathbb{K}[x,y].$$

Then the curve $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ defined by F intersects the line $x = 0$ exactly at the points $(0,0), (0,1), (0,\infty)$. The Newton diagrams of F at each of the three points are constituted of a unique segment with only two lattice points. Hence, F is necessarily non degenerate and locally irreducible at each point. In particular, the analytic factors are co-prime modulo x, and the Hensel lifting strategy leads to $\mathcal{C}(d_x, d_y) = \mathcal{O}(d_x d_y)$. Hence, the all rational factorization requires $\mathcal{O}(ab) = \mathcal{O}(d_x d_y)$ operations over $\mathbb{K}$ which has to be compared to the classical complexity bounds inherent to the choice of a regular fiber, namely $\mathcal{O}(d_x d_y s^{\omega-1})$ with s the number of rational places over a regular fiber [26]. Of course, the two complexities will be close as soon as s is small. The difference will be more remarkable in the absolute case for which a regular fiber imposes $s = d_y$ (see here after). In that example, we solve recombinations in the absolute case within $\mathcal{O}(d_x d_y)$ arithmetic operations over $\mathbb{K}$, while working over a regular fiber would lead to $\mathcal{O}(d_x d_y^\omega)$ operations over $\mathbb{K}$ [9].

Locally irreducible polynomials. This example motivates to introduce an important class of polynomials for which our approach leads to a good complexity. We say that F is locally irreducible along the line $x = 0$ (resp. absolutely locally irreducible) if the germs of curves $(C, P) \subset (\mathbb{P}^2_{\mathbb{K}}, P)$ defined by F are irreducible over $\mathbb{K}$ (resp. over $\bar{\mathbb{K}}$) at each rational place P of the line $x = 0$, including the place at infinity. For example, F is always locally irreducible along a regular fiber. The previous example is also such a polynomial.

Theorem 2. *There exists a deterministic algorithm that, given $F \in \mathbb{K}[x, y]$ absolutely locally irreducible along $x = 0$, returns its irreducible rational factorization with one factorization in $\mathbb{K}[y]$ of degree at most d_y plus*
- *$\mathcal{O}(d_x d_y s^{\omega-1})$ arithmetic operations over $\mathbb{K}$ if $p = 0$ or $p > d_x(2d_y - 1)$.*
- *$\mathcal{O}(k d_x d_y s^{\omega-1})$ arithmetic operations over $\mathbb{F}_p$ if $\mathbb{K} = \mathbb{F}_{p^k}$ and $p > d_y$.*

In the second case, it's enough to suppose that F is locally irreducible over $\mathbb{K}$.

Theorem 2 is not a direct application of Theorem 1 since we can have F locally irreducible with $q \approx d_x d_y$. This is for instance the case when the projective curve defined by F is a rational curve with a unique place along $x = 0$ and smooth outside this place. If F is non degenerate, checking local irreducibility has a negligible cost (Section 8). In general, this is more tricky. However, it has to be noticed that Abhyankar developed in [1] an algorithm for testing local irreducibility of a germ of curve that do not require blowing-ups or fractional power series (see also [10] for a generalization to positive characteristic). The main ingredient is that of *approximate roots* and the algorithm uses almost only resultant computations. Up to our knowledge, no complexity analysis have been done yet.

Counting factors and testing irreducibility. If we rather pay attention to the number of factors, it turns out that we need a lower truncation order ($\mathcal{O}(d_x)$ for fields of positive characteristic), leading to a better complexity. We say that $\mathbb{K}$ is an *absolute field* of F if it contains the field of definition of the irreducible absolute factors of F, that is, if rational and absolute factorizations coincide (as in the previous example).

Theorem 3. *(1) Suppose that $p = 0$. Then we can test irreducibility of a polynomial $F \in \mathbb{K}[x, y]$ satisfying hypothesis (H) with one factorization in $\mathbb{K}[y]$ of degree at most d_y plus*

$$\mathcal{O}(d_x d_y s^{\omega-1}) + \mathcal{C}(2d_x, d_y)$$

arithmetic operations over $\mathbb{K}$.

(2) Suppose that $p > 0$ or that $\mathbb{K}$ is an absolute field of F. We can compute the number of rational factors of $F \in \mathbb{K}[x, y]$ satisfying hypothesis (H) with one factorization in $\mathbb{K}[y]$ of degree at most d_y plus
- *$\mathcal{O}(d_x d_y s^{\omega-1}) + \mathcal{C}(d_x, d_y)$ operations over $\mathbb{K}$ if $p = 0$ or $p > d_x(2d_y - 1)$.*
- *$\mathcal{O}(k d_x d_y s^{\omega-1}) + \mathcal{O}(k)\mathcal{C}(d_x, d_y)$ operations over $\mathbb{F}_p$ if $\mathbb{K} = \mathbb{F}_{p^k}$.*

Note that we need not to suppose that $\mathbb{K}$ is an absolute field of F in the case of positive characteristic, leading in that case to a much stronger result. Roughly speaking, the underlying reason is that the Frobenius gives an efficient test for that an algebraic number in $\bar{\mathbb{K}}$ lies in the sub-field $\mathbb{K}$ (Section 5).

Absolute factorization. Finally, we apply our results to the problem of absolute factorization, that is factorization over $\bar{\mathbb{K}}$. Note that rational factorization can be seen as a subroutine of absolute factorization. Given $F \in \mathbb{K}[x,y]$ separable with respect to y, we represent the absolute factorization of F as a family of pairs

$$\{(P_1, q_1), \ldots, (P_t, q_t)\}$$

where $q_j \in \mathbb{K}[z]$ is separable, $P_j \in \mathbb{K}[x,y,z]$ satisfies $\deg_z P_j < \deg q_j$, the bi-degree of $P_j(x,y,\phi)$ is constant when ϕ runs over the roots of q_j and

$$F(x,y) = \prod_{j=1}^{t} \prod_{q_j(\phi)=0} P_j(x,y,\phi) \in \bar{\mathbb{K}}[x,y]$$

is the irreducible factorization of F in $\bar{\mathbb{K}}[x,y]$. This representation is not unique. We have that t is smaller or equal to the number r of irreducible rational factors, with equality if and only if the q_j's are irreducible. In analogy to the rational case, we denote by $\bar{r} = \sum \deg q_j$ the number of irreducible absolute factors of F. We represent the absolute analytic factorization of F in $\bar{\mathbb{K}}[[x]][y]$ exactly in the same way, the ring $\mathbb{K}[x]$ being replaced by $\mathbb{K}[[x]]$ (Section 7). We denote by $\bar{s}$ the number of irreducible analytic absolute factors of F, and we introduce $\bar{\mathcal{C}}(n, d_y)$ for the complexity of computing the n-truncated absolute analytic factorization of F.

Theorem 4. *Suppose that $p = 0$ or $p > d_x(2d_y - 1)$ and let $m := \max(q, d_x + 1)$. There exists a deterministic algorithm that, given $F \in \mathbb{K}[x,y]$ satisfying hypothesis (H), returns its absolute factorization with at most*

$$\mathcal{O}(m d_y \bar{s}^{\omega-1} + \bar{r} d_x d_y^2) + \bar{\mathcal{C}}(m, d_y) \subset \mathcal{O}(d_x d_y^{\omega+1}) + \bar{\mathcal{C}}(d_x d_y, d_y)$$

arithmetic operations over $\mathbb{K}$. We can take $m = d_x$ if F is locally absolutely irreducible along the fiber $x = 0$.

This result has to be compared to [9], Proposition 12, where the authors get complexity $\mathcal{O}(d^{\omega+1} + \bar{r} d_x d_y^2)$ for absolute factorization, where d is the total degree of F. Note that in contrast to Theorem 1, we assume here that $\mathbb{K}$ has cardinality greater or equal to $d_x(2d_y - 1)$. If we only pay attention to the number of absolutely irreducible factors, we can avoid this hypothesis and we can deal with the only $(d_x + 1)$-truncation order.

Theorem 5. *There exists a deterministic algorithm that, given $F \in \mathbb{K}[x,y]$ satisfying hypothesis (H), returns the number $\bar{r}$ of irreducible absolute factors of F with at most*

- *$\mathcal{O}(d_x d_y \bar{s}^{\omega-1}) + \mathcal{C}(d_x, d_y)$ operations over $\mathbb{K}$ if $p = 0$ or $p > d_x(2d_y - 1)$.*
- *$\mathcal{O}(k d_x d_y \bar{s}^{\omega-1}) + \mathcal{O}(k)\mathcal{C}(d_x, d_y)$ operations over $\mathbb{F}_p$ if $\mathbb{K} = \mathbb{F}_{p^k}$.*

This result has to be compared to [9], Proposition 12, where the authors get complexity $\mathcal{O}(d^{\omega+1})$ for computing the number of irreducible absolute factors. As mentioned already, the great advantage of our algorithm is that, when working over a regular fiber, the number of absolute analytic factors to recombine is always d_y, while working over critical fibers reduces this number to $\bar{s} \leq d_y$. More precisely, if e_i and f_i stand respectively for

the ramification indices and residue degrees of the s rational places of C over $\mathbb{K}$, the difference between $\bar{s}$ and d_y is measured by the formulas

$$\bar{s} = \sum_{i=1}^{r} f_i \quad \leq \quad d_y = \sum_{i=1}^{r} e_i f_i.$$

Hence, the more ramified the fiber is, the more we gain during the recombination step. Of course, in counterpart, we have to perform analytic factorization along a critical fiber.

Example. Here is a very simple illustrating example. Suppose for instance that

$$F = (y^a + \sqrt{2}x^b + x^b y^a)(y^a - \sqrt{2}x^b + x^b y^a)$$

for some co-prime integers a, b. Then, the curve $F = 0$ has only one rational place over $x = 0$, with ramification index $e = a$ and residual degree $f = 2$. Moreover, F is non degenerate with respect to its Newton polytope. It follows in particular that $m = d_x + 1$. After some monomial change of coordinates, we can apply an absolute Hensel lifting strategy which leads to $\bar{\mathcal{C}}(d_x) \subset \mathcal{O}(d_x d_y)$. Since both $\bar{s}$ and $\bar{r}$ are constant, it follows from Theorem 4 and 5 that we compute the number of absolute factors and the absolute factorization of F with respective complexities $\mathcal{O}(d_x d_y)$ and $\mathcal{O}(d_x d_y^2)$, which have to be compared to the complexities $\mathcal{O}(d_x d_y^\omega)$ inherent to the choice of a regular fiber [9]. For instance, taking $x = 1$ leads to $F(1, y) = 4y^{2a} - 2$. This polynomial is separable, and the algorithm in [9] would have lift the factors of $F(1, y)$ up to precision $d_x + 1$ and then recombine them, leading to the complexity $\mathcal{O}(d_x d_y^\omega)$. Note moreover that the strong sparsness of F would have been broken after the change of variable $x \to x + 1$. Of course, this is a very special example. In general, it would be interesting to know both in practice and in theory which approach is the best one.

Main line of the proofs. The approach we propose to solve the problem of recombinations of analytic factors follows closely that of Lecerf [26]. Namely, we use logarithmic derivatives in order to reduce a multiplicative recombination problem to an additive recombination problem. Then, a simple observation shows that we need to test if some rational function G/F has all its residues ρ_k's in the sub-field $\bar{\mathbb{K}} \subset \overline{\mathbb{K}(x)}$, a problem that can be reduced to a divisibility test by F for zero or big enough characteristic. Note that in contrast to [26], we do not make any assumption on the cardinality of the field so that we need to take care to the case when the leading coefficient of F is not invertible in $\mathbb{K}[[x]]$. For small positive characteristic, we test x-independence of the residues thanks to an $\mathbb{F}_p$-linear operator introduced by Niederreiter for univariate factorization [27] and extended to the bivariate case by Lecerf [26]. Hence, linear algebra over $\mathbb{F}_p$ appears, explaining that our complexity results are expressed only for finite fields when the characteristic is small. When the fiber is regular, residues in $\bar{\mathbb{K}}$ turn out to be a sufficient condition for solving recombinations. Along a critical fiber, this is not the case any more. The basic idea is to introduce extra linear equations that depend on the higher truncated analytic factors. To this aim, we introduce the *separability order* of F which in the monic case, coincides with the maximal x-valuation of $\partial_y F(x, \phi)$ when ϕ runs over the roots of F. We show that this integer gives an upper bound for the required precision. If we know moreover that the residues of G/F lie in the sub-field $\mathbb{K} \subset \bar{\mathbb{K}}$, we show that we can improve this upper bound. This is the kind of arguments that allows us to prove (2) in Theorem 3. Finally, we extend our results to the absolute case by using a Vandermonde matrix that allows to reduce $\bar{\mathbb{K}}$-linear algebra to $\mathbb{K}$-linear algebra.

Organization of the paper. In Section 2, we introduce our main notations and we explain the recombination problem. In Section 3, we solve the recombination problem along a critical fiber. In Section 4, we pay attention to the subproblem of counting the number of factors and we give in particular an irreducibility test. We discuss moreover some combinatorial approaches for solving recombinations of some so-called reasonably ramified polynomials. In Section 5, we give explicit equations for constant residues, mainly following [26]. In Section 6, we develop the algorithms underlying Theorem 1 and 3 and we study their complexities. We consider the case of locally irreducible polynomials and we prove Theorem 2 in Subsection 6.3. In Section 7, we pay attention to absolute factorization and we prove theorems 4 and 5. In Section 8, we consider the case of non degenerate polynomials with respect to their P-adic Newton polytopes. We conclude in Section 9.

2. Factorization, recombinations, residues.

We explain here the strategy developed by Lecerf in [26] for solving recombinations in the regular case, and we show that some problems occur when working along a critical fiber. For convenience to the reader, we tried to follow the notations of [26]. In all of this section, we suppose that F is primitive with respect to y, a situation that can be reached with a negligible cost for our purpose. For convenience, we only pay attention to rational factorization, the absolute case being treated separately in Section 7.

2.1. The recombination problem

We normalize F by requiring that its leading coefficient with respect to y has its first non zero coefficient equal to 1. The polynomial F thus admits a unique rational factorization

$$F = F_1 \cdots F_r \in \mathbb{K}[x, y], \tag{1}$$

where each $F_j \in \mathbb{K}[x, y]$ is irreducible, with leading coefficient with first non zero coefficient equal to 1. Also, F admits a unique analytic factorization of the form

$$F = u\mathcal{F}_1 \cdots \mathcal{F}_s \in \mathbb{K}[[x]][y] \tag{2}$$

where the $\mathcal{F}_i \in \mathbb{K}[[x]][y]$ are irreducible with leading coefficient x^{n_i}, $n_i \in \mathbb{N}$ and $u \in \mathbb{K}[x]$, $u(0) \neq 0$. Hence, each rational factor F_j has a unique normalized factorization

$$F_j = c_j \mathcal{F}_1^{v_{j1}} \cdots \mathcal{F}_r^{v_{jr}}, \quad j = 1, \ldots, r. \tag{3}$$

for some polynomial $c_j \in \mathbb{K}[x]$, $c_j(0) = 1$. The recombination problem consists to compute the exponent vectors

$$v_j = (v_{j1}, \ldots, v_{jr}) \in \mathbb{N}^r$$

for all $j = 1, \ldots, r$. Then, the computation of the F_j's follows easily. Since F is separable by hypothesis, the vectors v_j form a partition of $(1, \ldots, 1)$ of length r. In particular, they form up to reordering the reduced echelon basis of the vector subspace they generate over any given field $\mathbb{F}$. In positive characteristic, our algorithm will have to solve linear equations both over $\mathbb{K}$ and over $\mathbb{F}_p$. Hence, in order to unify our notations, we consider for a while the recombination problem over $\mathbb{F}$ a fixed given sub-field of $\mathbb{K}$. Namely, we want to compute a basis of the following $\mathbb{F}$-vector space

$$S := \langle v_1, \ldots, v_r \rangle_{\mathbb{F}} \subset \mathbb{F}^s.$$

Hence, solving recombinations essentially reduces to finding a system of $\mathbb{F}$-linear equations that determine $S \subset \mathbb{F}^s$. If not specified, all vector spaces we introduce from now are defined over $\mathbb{F}$, keeping in mind that $\mathbb{F}$ will have to play the role of $\mathbb{K}$ or $\mathbb{F}_p$.

Truncated functions. Given $\mathcal{G} \in \mathbb{K}[[x]][y]$, we denote by $[\mathcal{G}]^n \in \mathbb{K}[x,y]$ the canonical representative of $\mathcal{G}$ modulo (x^n). We call it the n-truncation of $\mathcal{G}$. We will use also the notation

$$[\mathcal{G}]_n := \mathcal{G} - [\mathcal{G}]^n \qquad \text{and} \qquad [\mathcal{G}]_n^m := [\mathcal{G}]^m - [\mathcal{G}]^n$$

for lower truncation of functions, with convention that $[\mathcal{G}]_n^m = 0$ for $n \geq m$. In other words, we put to zero all coefficients of monomials with x-degree $< n$.

2.2. Recombination and residues.

The key point to solve recombinations is to reduce a multiplicative problem to a linear algebra problem thanks to the logarithmic derivative operator. Let $\hat{\mathcal{F}}_i$ stands for the quotient of F by $\mathcal{F}_i$. Let $\mu = (\mu_1, \ldots, \mu_s) \in \mathbb{F}^s$. Applying logarithmic derivative with respect to y to (3) and multiplying by F we get the key characterization

$$\mu \in S \iff \exists\, \alpha_1, \ldots, \alpha_r \in \mathbb{F} \quad | \quad \sum_{i=1}^{s} \mu_i \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i = \sum_{j=1}^{r} \alpha_j \hat{F}_j \partial_y F_j. \tag{4}$$

The reverse implication holds thanks to the separability assumption on F ([26], Lemma 1). The key idea is to derive from (4) a system of linear equations for S that depends only on the (d_x+1)-truncated polynomial

$$G_\mu := \sum_{i=1}^{s} \mu_i \big[\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i\big]^{d_x+1} \in \mathbb{K}[x,y].$$

Let $G = G_\mu$ and let us denote by $\rho_k = \rho_k(\mu)$ the residues

$$\rho_k := \frac{G(x, y_k)}{\partial_y F(x, y_k)} \in \overline{\mathbb{K}(x)}, \qquad k = 1, \ldots, d_y$$

of G/F at the roots $y_k \in \overline{\mathbb{K}(x)}$ of F. These residues are well defined thanks to the separability assumption on F. We get from (4) that

$$\mu \in S \implies \rho_k \in \mathbb{F} \quad \forall\, k = 1, \ldots, d_y. \tag{5}$$

In particular, we have an inclusion of $\mathbb{F}$-vector spaces

$$S \subset V(\mathbb{L}) := \Big\{ \mu \in \mathbb{F}^s \mid \rho_k \in \mathbb{L},\ k = 1, \ldots, d_y \Big\}$$

for any sub-field $\mathbb{L} \subset \overline{\mathbb{K}(x)}$. In the regular case, the reverse inclusion holds as soon as $\mathbb{L} \subset \bar{\mathbb{K}}$, thanks to the following proposition ([26], Lemma 2).

Proposition 2.1. *Suppose that $F(0,y)$ is separable of degree d_y. Then $S = V(\bar{\mathbb{K}})$.*

In characteristic zero or high enough, we get that $\mu \in S$ if and only if $\rho_k' = 0$ for all k, a condition that can be translated into a finite number of linear equations over $\mathbb{K}$. In small positive characteristic p, we have that $\rho_k' = 0$ implies that $\rho_k \in \overline{\mathbb{K}(x^p)}$ and we use then the Niederreiter operator in order to get some extra $\mathbb{F}_p$-linear equations that allow to test $\rho_k \in \bar{\mathbb{K}}$ (see Section 3).

Unfortunately, the equality $S = V(\bar{\mathbb{K}})$ in Proposition 2.1 no longer holds along a critical fiber, as illustrated by the following example.

Example 2.2. Let $F = y^6 - (y-x)^2 \in \mathbb{Q}[x,y]$. We see that $F(0,y)$ has a double root so that the fiber $x = 0$ is critical. We compute that F has $s = 5$ irreducible analytic factors over $\mathbb{Q}$ and $r = 2$ rational factors. Two of the analytic factors of F have x-adic expansions

$$\mathcal{F}_1 = y - x - x^3 + \cdots, \qquad \mathcal{F}_2 = y - x + x^3 + \cdots$$

Since $d_x = 2$, it follows that

$$[\hat{\mathcal{F}}_1 \partial_y \mathcal{F}_1]^{d_x+1} = [\hat{\mathcal{F}}_2 \partial_y \mathcal{F}_2]^{d_x+1}.$$

In particular, the vector $\mu = (1,-1,0,0,0) \in \mathbb{F}^5$ gives the zero polynomial $G_\mu = 0$, hence the trivial relation $\mu \in V(\bar{\mathbb{Q}})$. We can check that $\mu \notin S$ so that Proposition 2.1 doesn't hold in that case.

This example suggests to quotient $V(\bar{\mathbb{K}})$ by the vector subspace Z of relations $G_\mu = 0$. Unfortunately, we could not prove that the isomorphism $S \simeq V(\bar{\mathbb{K}})/Z$ always hold, although this is the kind of approach we will follow in order to compute the number of irreducible factors (Subsection 4.1). Moreover, even if such an isomorphism holds, it does not allow in general to compute the reduced echelon basis of S thanks to linear algebra (see Subsection 4.4). Hence, we rather prefer to reduce recombinations to linear algebra. To do so, we need to introduce extra equations for S. Not surprisingly, these equations will depend now on the analytic factors of F truncated up to some higher precision, this precision being closely related to the valuation of the discriminant.

3. Recombinations along a critical fiber

In Subsection 3.1, we introduce the notion of separability order of F. This integer will measure how much the fiber $x = 0$ is critical for F and will play the role of an upper bound for the truncation order of the analytic factors. In Subsection 3.2, we solve the recombination problem along a critical fiber. We keep the same notations and hypothesis as in the previous section. In particular, F is primitive with respect to y.

3.1. The separability order

To each analytic factor $\mathcal{F}_i$ of F, we associate the integers

$$r_i := \operatorname{val}_x \operatorname{Res}_y(\mathcal{F}_i, \hat{\mathcal{F}}_i), \qquad \delta_i := \operatorname{val}_x \operatorname{Disc}_y(\mathcal{F}_i), \qquad d_i := \deg_y(\mathcal{F}_i).$$

Here, Res_y and Disc_y stand for the usual resultants and discriminants with respect to y, and val_x stands for the x-adic valuation of $\mathbb{K}[[x]]$. We introduce the rational number

$$q_i := \frac{r_i + \delta_i}{d_i}$$

and we denote by $N = N(F)$ the integer:

$$N := \max\left\{\lfloor q_1 \rfloor, \ldots, \lfloor q_r \rfloor\right\}.$$

The integer N measures in some sense how critical the fiber $x = 0$ is for the curve $F = 0$. We call it the *separability order* of F along the fiber $x = 0$. In particular, we have $N = 0$ if $F(0,y)$ is separable of degree d_y (the converse is false, take for instance $F = y^2 - x$). The integer N will play the role of an upper bound for the truncation order that allows

to solve recombinations. The following lemma summarizes its main properties. We recall that the standard x-adic valuation val_x of the complete field $\mathbb{K}((x))$ uniquely extends to a valuation on its algebraic closure $\overline{\mathbb{K}((x))}$, that we still denote by val_x.

Lemma 3.1. *(1) We have equality*

$$q_1 d_1 + \cdots + q_s d_s = \mathrm{val}_x \operatorname{Disc}_y(F). \tag{6}$$

(2) Let ϕ be a root of $\mathcal{F}_i$, and denote by n_i the x-valuation of the leading coefficient of $\mathcal{F}_i$. We have the relation

$$q_i = \mathrm{val}_x\, \partial_y F(\phi) + \frac{(d_y - 2)n_i}{d_i}. \tag{7}$$

In particular, if the leading coefficient of F is invertible in $\mathbb{K}[[x]]$, we have that

$$\{q_1, \ldots, q_s\} = \big\{ \mathrm{val}_x\, \partial_y F(\phi),\ \phi \text{ roots of } F\big\}.$$

Proof. By the multiplicative properties of the discriminant and the resultant, we get that

$$\begin{aligned}\operatorname{Disc}_y(F) &= \prod_{i=1}^{s} \operatorname{Disc}_y(\mathcal{F}_i) \prod_{1\le i<j\le s} \operatorname{Res}_y(\mathcal{F}_i, \mathcal{F}_j)^2 \\ &= \prod_{i=1}^{s} \operatorname{Disc}_y(\mathcal{F}_i) \prod_{i=1}^{s} \operatorname{Res}_y(\mathcal{F}_i, \hat{\mathcal{F}}_i),\end{aligned}$$

and (1) follows directly by applying val_x to this equality. Let now ϕ be a root of $\mathcal{F}_i$. On the one hand we have

$$\partial_y F(\phi) = \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i(\phi)$$

and on the other hand, we have the product formula

$$\prod_{\mathcal{F}_i(\phi)=0} \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i(\phi) = \operatorname{Res}_y(\mathcal{F}_i, \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i)\, \mathrm{lc}(\mathcal{F}_i)^{1-d_y},$$

where $\mathrm{lc}(\mathcal{F}_i)$ stands for the leading coefficient of $\mathcal{F}_i$ and where the left hand side product runs over all roots of $\mathcal{F}_i$. Combined with the multiplicative property of the resultant

$$\operatorname{Res}_y(\mathcal{F}_i, \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i) = \operatorname{Res}_y(\mathcal{F}_i, \hat{\mathcal{F}}_i)\, \operatorname{Res}_y(\mathcal{F}_i, \partial_y \mathcal{F}_i)$$

and with its relation to the discriminant

$$\operatorname{Res}_y(\mathcal{F}_i, \partial_y \mathcal{F}_i) = \mathrm{lc}(\mathcal{F}_i)\, \operatorname{Disc}_y(\mathcal{F}_i),$$

we get the formula

$$\prod_{\mathcal{F}_i(\phi)=0} \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i(\phi) = \mathrm{lc}(\mathcal{F}_i)^{2-d_y} \operatorname{Res}_y(\mathcal{F}_i, \hat{\mathcal{F}}_i)\, \operatorname{Disc}_y(\mathcal{F}_i).$$

Since val_x is invariant under the $\mathbb{K}((x))$-automorphisms of the algebraic closure of $\mathbb{K}((x))$, point (2) follows by applying val_x to the previous equality and by dividing by the degree d_i of $\mathcal{F}_i$. □

Remark 3.2. Lemma 3.1 implies in particular that

$$N \leq \frac{\mathrm{val}_x \mathrm{Disc}_y(F)}{d} \leq \frac{d_x(2d_y-1)}{d},$$

where $d := \min\{d_i,\, i=1,\dots,s\}$ stands for the minimal degree of the $\mathcal{F}_i$'s. In particular, $N \in \mathcal{O}(d_x d_y)$. The following generalization of Example 2.2, suggested to us by Eduardo Casas-Alvero, shows that N may reach this order of magnitude.

Example 3.3. Let $F(x,y) := (y-x^m)^2 + y^n \in \mathbb{Q}[x,y]$, with $n \geq 3$ odd. Then $(0,0)$ is the unique point of the curve $F=0$ that is ramified over $x=0$. We can show that F admits a unique irreducible analytic factor $\mathcal{F}_1$ vanishing at $(0,0)$, with degree $d_1 = 2$. It follows that

$$\delta_1 = \mathrm{val}_x \mathrm{Disc}_y(F) \quad \text{and} \quad r_1 = 0,$$

while $\delta_i = r_i = 0$ for all $i > 1$. We compute here that $\mathrm{val}_x \mathrm{Disc}_y(F) = mn$. It follows that

$$N = \Big\lfloor \frac{r_1+\delta_1}{d_1} \Big\rfloor = \Big\lfloor \frac{mn}{2} \Big\rfloor = \Big\lfloor \frac{d_x d_y}{4} \Big\rfloor,$$

which is of the order of magnitude of $d_x d_y$.

3.2. Solving recombinations along a critical fiber.

We can derive from (4) an other obvious source of equations for S. Namely, let us introduce for $n \in \mathbb{N}$ the $\mathbb{F}$-vector subspace

$$W^n := \Big\{ \mu \in \mathbb{F}^s \;\mid\; \sum_{i=1}^{s} \mu_i \big[\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i\big]_{d_x+1}^{n} = 0 \Big\},$$

with convention $W^n = \mathbb{F}^s$ when $n \leq d_x + 1$. For a question of degree, (4) implies that we have the inclusions

$$S \subset W^n \quad \forall n \in \mathbb{N}.$$

Our next result ensures that the separability order gives an *a priori* upper bound for n for which W^n provides enough extra equations to solve the recombination problem.

Theorem 3.4. *We have $S = V(\bar{\mathbb{K}}) \cap W^n$ for all $n > N$.*

In particular, if $N \leq d_x$, then the recombinations are solved by the same system of linear equations as in the regular case:

Corollary 3.5. *Suppose that $N \leq d_x$. Then $S = V(\bar{\mathbb{K}})$.*

Remark 3.6. This corollary implies in particular that all polynomials that are non degenerate with respect to their Newton polytope satisfy $V(\bar{\mathbb{K}}) = S$ (see Section 8).

Remark 3.7. Suppose that F is separable with respect to y. For $\alpha \in \mathbb{P}^1_{\mathbb{K}}$, let us denote by N_α the separability order of F over the fiber $x=\alpha$. From inequalities,

$$\sum_{\alpha \in \mathbb{P}^1_{\mathbb{K}}} N_\alpha \leq \sum_{\alpha \in \mathbb{P}^1_{\mathbb{K}}} \mathrm{val}_{x-\alpha} \mathrm{Disc}_y(F) = \deg_x \mathrm{Disc}_y(F) \leq d_x(2d_y-1),$$

we deduce that there always exist a fiber for which $N_\alpha \leq d_x$ as soon as $\mathbb{K}$ has cardinality $\geq 2d_y - 3$.

In order to prove Theorem 3.4, we need to prove two preliminary results. The first key lemma will be used many times in the paper.

Lemma 3.8. *Let $\mathbb{K} \subset \mathbb{L} \subset \overline{\mathbb{K}((x))}$ be a field and let $G \in \mathbb{K}[x,y]$, with $\deg_y G < d_y$. The residues ρ_k of G/F all lie in $\mathbb{L}$ if and only if G is $\mathbb{L}$-linear combination of the $\hat{E_j}\partial_y E_j$'s, where the E_j's stand for the irreducible factors of F over $\mathbb{L}$.*

Proof. One direction is clear: if $G = \sum \alpha_j \hat{E_j} \partial_y E_j$, then $\rho_k = \alpha_j \in \mathbb{L}$ where j is determined by condition $E_j(x, y_k) = 0$. Suppose now that $\rho_k \in \mathbb{L}$. Thanks to the degree assumption on G and the separability assumption on F, we have the partial fraction decomposition

$$\frac{G}{F} = \sum_{k=1}^{d_y} \frac{\rho_k}{y - y_k}.$$

Let $\tau \in \Gamma := \mathrm{Aut}\left(\overline{\mathbb{L}(x)}/\mathbb{L}(x)\right)$ acts on this equality. By assumption, τ leaves both G/F and ρ_k fixed. Hence, we get

$$\sum_{k=1}^{d_y} \frac{\rho_k}{y - \tau(y_k)} = \sum_{k=1}^{d_y} \frac{\rho_k}{y - y_k} = \sum_{k=1}^{d_y} \frac{\rho_{k_\tau}}{y - \tau(y_k)},$$

the second equality using that τ permutes the roots of F. Here, the notation k_τ stands for the unique index such that $\phi_{k_\tau} = \tau(y_k)$. The partial fraction decomposition being unique, previous equality implies that

$$\rho_k = \rho_{k_\tau} \quad \forall\, \tau \in \Gamma.$$

Since Γ acts transitively on the set of roots of each $\mathbb{L}$-irreducible factor E_j, it follows that $\rho_k = \rho_{k'}$ whenever $E_j(x, y_k) = E_j(x, y_{k'}) = 0$. Hence, there exist constants $\alpha_1, \ldots, \alpha_\ell \in \mathbb{L}$ such that

$$\frac{G}{F} = \sum_{j=1}^{\ell} \alpha_j \Big(\sum_{k | E_j(y_k)=0} \frac{1}{y - y_k} \Big) = \sum_{j=1}^{\ell} \alpha_j \frac{\partial_y E_j}{E_j}.$$

The result follows from multiplication by F. □

The next lemma computes the valuations of the roots of F.

Lemma 3.9. *Let $\mathcal{F} \in \mathbb{K}[[x]][y]$ be an irreducible polynomial of degree d in y. Let a and b stand respectively for the valuation of the leading coefficient and the constant coefficient of $\mathcal{F}$ seen as a polynomial in y. Let $\phi \in \overline{\mathbb{K}((x))}$ be a root of $\mathcal{F}$. Then $\mathrm{val}_x(\phi) = (b-a)/d$ and either a or b is equal to 0.*

Proof. Since $\mathcal{F}$ is irreducible, at least one of its coefficient has valuation 0. Hence, if both a and b are non zero, then its Newton polytope would contain at least two distinct compact edges (Section 8). This is impossible since $\mathcal{F}$ is irreducible. Let N stands for the norm of the field extension of $\mathbb{K}((x))$ defined by $\mathcal{F}$. Then $\mathrm{N}(\phi)$ is equal to the quotient of the constant coefficient of $\mathcal{F}$ by its leading coefficient. Hence $\mathrm{val}_x \mathrm{N}(\phi) = b - a$ and we conclude thanks to the relation $\mathrm{val}_x \phi = \mathrm{val}_x \mathrm{N}(\phi)/\deg(\phi)$. □

Proof of Theorem 3.4. We already saw that $S \subset V(\bar{\mathbb{K}}) \cap W^n$ and we need to prove the reverse inclusion when $n > N$. Let $\mu \in V(\bar{\mathbb{K}}) \cap W^n$. Thanks to the previous lemma, and by definition of W^n, we deduce that there exists some constants $\alpha_j \in \bar{\mathbb{K}}$ such that

$$\sum_{i=1}^{s} \mu_i \big[\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i\big]^m = \sum_{j=1}^{\ell} \alpha_j \hat{E}_j \partial_y E_j, \tag{8}$$

where $m = \max(d_x + 1, n)$ and where the E_j's stand for the irreducible factors of F over $\bar{\mathbb{K}}$. Let $\phi \in \overline{\mathbb{K}((x))}$ be a root of $\mathcal{F}_i$ and let j be the unique index such that $E_j(\phi) = 0$. Using the relations

$$\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i(\phi) = \hat{E}_j \partial_y E_j(\phi) = \partial_y F(\phi),$$

we get by evaluating (8) at ϕ an equality

$$(\mu_i - \alpha_j)\partial_y F(\phi) = x^m R(\phi) \tag{9}$$

for some $R \in \mathbb{K}[[x]][y]$. We need a lower bound on the valuation of $R(\phi)$. We remark that the coefficient of $y^{d_y - 1}$ in $\partial_y \mathcal{F}$ is equal to $d_y \operatorname{lc}_y(F)$. Since the leading coefficient of F is a polynomial in x of degree at most d_x, equation (9) implies that R has y-degree $\leq d_y - 2$. Hence, ultrametric inequality combined with Lemma 3.9 gives

$$\operatorname{val}_x R(\phi) \geq \min\{\operatorname{val}_x \phi^i,\ i = 0, \ldots, d_y - 2\} \geq -\frac{(d_y - 2)n_i}{d_i},$$

(recall that x^{n_i} stands for the leading coefficient of $\mathcal{F}_i$). Suppose that $\mu_i \neq \alpha_j$. Hence, (9) gives

$$\operatorname{val}_x \partial_y F(\phi) \geq m - \frac{(d_y - 2)n_i}{d_i}.$$

By Lemma 3.1, this is equivalent to that $m \leq q_i$, contradicting our hypothesis $m = \max(d_x + 1, n) > N$. It follows that $\mu_i = \alpha_j$. Combined with (8), we get that

$$G := \Big[\sum_{i=1}^{s} \mu_i \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i\Big]^{d_x+1} = \sum_{i=1}^{s} \mu_i \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i.$$

In particular, the residues of G/F all lie in $\mathbb{F} \subset \mathbb{K}$, and it follows from Lemma 3.8 that

$$G = \sum_{i=s}^{r} \mu_i \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i = \sum_{j=1}^{r} c_j \hat{F}_j \partial_y F_j.$$

for some $c_j \in \mathbb{K}$. Since $\mathcal{F}_i$ is co-prime to $\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i$ by hypothesis, this relation forces equality $\mu_i = c_j$ when $\mathcal{F}_i$ divides F_j. It follows that $\mu \in S$. □

Remark 6. As an optimization, the vector subspace W^n may be defined to depend on the Newton polytope instead of partial degrees. Namely, it's enough to look for linear combinations $\sum_i \mu_i \big[\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i\big]^n$ whose Newton polytope is contained in that of $\partial_y F$.

4. Counting the number of irreducible factors

We show here how to bound the number of factors with the $d_x + 1$-truncation order and we deduce a deterministic irreducibility test that requires the only $2d_x$-truncation order. We still suppose that F is primitive with respect to y.

4.1. An upper bound for the number of factors

Example 2.2 suggests to introduce the vector subspace Z of vectors μ whose associated truncated polynomial G_μ is zero, that is

$$Z := \Big\{\mu \in \mathbb{F}^s \mid \sum_{i=1}^{s} \mu_i \big[\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i\big]^{d_x+1} = 0\Big\}.$$

We have the following result.

Proposition 4.1. *We have $V(\mathbb{F}) = S \oplus Z$.*

Proof. We already saw that $S \subset V(\mathbb{F})$, while the inclusion $Z \subset V(\mathbb{F})$ trivially holds. Hence, we get an inclusion $S + Z \subset V(\mathbb{F})$. Let us show the reverse inclusion. If $\mu \in V(\mathbb{F})$, it follows from Lemma 3.8 that G_μ is $\mathbb{F}$-linear combinations of the irreducible factors of F over $\mathbb{K}$. It follows that

$$\sum_{i=1}^{s} \mu_i [\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i]^{d_x+1} = \sum_{i=1}^{s} \alpha_i [\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i]^{d_x+1},$$

for some $\alpha = (\alpha_1, \ldots, \alpha_s) \in S$. In particular, $\mu - \alpha \in Z$. Equality $V(\mathbb{F}) = S + Z$ follows. Finally, if $\mu \in S \cap Z$ we get that

$$\sum_{i=1}^{s} \mu_i \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i = \sum_{i=1}^{s} \mu_i \big[\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i\big]^{d_x+1} = 0,$$

so that $\mu = 0$ by linear independence of the $\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i$'s. It follows that $V(\mathbb{F}) = S \oplus W$. □

Remark 4.2. We have $Z = 0$ as soon as the separability order satisfies $N \leq d_x + 1$. Namely, we have in that case $S = V(\bar{\mathbb{K}})$ by Theorem 3.4 and we conclude thanks to the inclusion $S \oplus Z = V(\mathbb{K}) \subset V(\bar{\mathbb{K}})$.

For fields of positive characteristic, we can take $\mathbb{F}$ as the prime field of $\mathbb{K}$, in which case the Niederreiter operator leads to an explicit system of equations for $V(\mathbb{F})$ (see Section 5). Hence, Proposition 4.1 allows to compute the number of irreducible factors

$$r = \dim_{\mathbb{F}} V(\mathbb{F}) - \dim_{\mathbb{F}} Z$$

with linear algebra from the $(d_x + 1)$-truncated analytic factors only. For fields of characteristic zero, testing whether the residues lie in $\mathbb{K}$ is a much harder task. In that case, we only get equations for $V(\bar{\mathbb{K}})$, so that Proposition 4.1 *a priori* allows only to compute the upper bound

$$r \leq \dim_{\mathbb{F}} V(\bar{\mathbb{K}}) - \dim_{\mathbb{F}} Z.$$

This problem motivates to explore in more details the relations between $V(\mathbb{F})$ and $V(\bar{\mathbb{K}})$.

4.2. On the relations beetween $V(\mathbb{F})$ and $V(\bar{\mathbb{K}})$

In regards to the Proposition 4.1, we may ask whether equality $V(\mathbb{F}) = V(\bar{\mathbb{K}})$ holds. We could not prove nor disprove this equality. However, we give here some conditions under which it holds. Let us first note the following lemma.

Lemma 4.3. *If all the absolute factors of F are defined over $\mathbb{K}$, then $V(\mathbb{K}) = V(\bar{\mathbb{K}})$.*

Proof. By Lemma 3.8, if $\mu \in V(\bar{\mathbb{K}})$, then $G_\mu = \sum \alpha_j \hat{E}_j \partial_y E_j$ for some $\alpha_j \in \bar{\mathbb{K}}$, and where the E_j's stand for the irreducible absolute factors of F. By assumption, we have that $E_j \in \mathbb{K}[x]$. Applying $\tau \in \mathrm{Aut}_{\mathbb{K}}(\bar{\mathbb{K}})$ to the previous equality, and using that G_μ has coefficients in $\mathbb{K}$, we get that

$$\sum_j \tau(\alpha_j) \hat{E}_j \partial_y E_j = \sum_j \alpha_j \hat{E}_j \partial_y E_j,$$

which implies that $\tau(\alpha_j) = \alpha_j$ by $\bar{\mathbb{K}}$-linear independence of the $\hat{E}_j \partial_y E_j$'s. This being true for all τ, it follows that $\alpha_j \in \mathbb{K}$. Hence $\mu \in V(\mathbb{K})$ by Lemma 3.8. $\square$

To each rational factor F_j of F, we associate the integer

$$M_j := \min\Big\{ \lfloor q_i \rfloor,\ \mathcal{F}_i \text{ divides } F_j \text{ in } \mathbb{K}[[x]][y] \Big\}.$$

Roughly speaking, M_j measures the minimal contact order of the curve $F_j = 0$ with the complementary curve $\hat{F}_j = 0$ along the line $x = 0$. We denote by

$$M := \max\{M_j,\ j = 1, \dots, r\}.$$

Note the obvious relation $M \leq N$ with the separability order.

Proposition 4.4. *We have $V(\bar{\mathbb{K}}) \cap W^n = V(\mathbb{F}) \cap W^n$ for all $n > M$.*

Proof. The proof is similar to that of Theorem 3.4. Let $n > M$ and denote by $m := \max\{n, d_x + 1\}$. By Lemma 3.8 and by definition of W^n we have $\mu \in V(\bar{\mathbb{K}}) \cap W^n$ if and only if

$$\sum_{i=1}^{s} \mu_i [\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i]^m = \sum_{k=1}^{t} \alpha_k \hat{E}_k \partial_y E_k, \tag{10}$$

where the $E_k \in \bar{\mathbb{K}}[x, y]$ stand for the absolutely irreducible factors of F. Let us fix F_j a rational factor of F. By assumption, there exists $\mathcal{F}_i$ a divisor of F_j such that $q_i \leq n$. Let E_k be a divisor of F_j. Then E_k shares at least one root $\phi \in \overline{\mathbb{K}(x)}$ with $\mathcal{F}_i$. Hence, by evaluating (10) at ϕ we get that

$$(\mu_i - \alpha_k) \partial_y F(\phi) = x^m R(\phi)$$

for some $R \in \mathbb{K}[[x]][y]$. Taking x-valuations, and reasonning as in the proof of Theorem 3.4, we get that $\mu_i \neq \alpha_k$ implies $q_i \geq m$, a contradiction. Hence $\alpha_k = \mu_i \in \mathbb{F}$ for all irreducible factors E_k of F_j. Repeating this reasoning for all factors F_j of F, we deduce by regrouping the factors E_k by conjugacy classes that we have

$$\sum_{i=1}^{s} \mu_i [\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i]^m = \sum_{j=1}^{s} c_j \hat{F}_j \partial_y F_j,$$

for some c_j's in $\mathbb{F}$. For a degree reason, this is equivalent to that

$$\sum_{i=1}^{s} \mu_i [\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i]^{d_x+1} = \sum_{j=1}^{s} c_j \hat{F}_j \partial_y F_j \quad \text{and} \quad \sum_{i=1}^{s} \mu_i [\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i]^m_{d_x+1} = 0$$

The first equation is equivalent to that $\mu \in V(\mathbb{F})$ by Lemma 3.8, while second equation is equivalent to that $\mu \in W^n$ by definition. $\square$

Last Proposition says in particular that if each irreducible rational factor of F has at least one branch with $q_i \leq d_x$, then we have $V(\bar{\mathbb{K}}) = V(\mathbb{F})$. This is the case for instance in Example 2.2, Section 2. Here is a trivial example that illustrates that the converse doesn't hold.

Example 4.5. Let $F(x,y) = ((y-x)^2 + y^{10})(y-x) \in \mathbb{Q}[x,y]$. Then F has exactly 3 anaytic factors over $\mathbb{Q}$ which satisfy

$$\mathcal{F}_1 \equiv (y-x)^2 \mod x^4, \quad \mathcal{F}_2 \equiv y - x \mod x^4, \quad \mathcal{F}_3 = y^8 + 1 + \cdots .$$

We find here that $q_1 = q_2 = 10$. In particular, the rational factor $y - x$ of F has a unique branch $\mathcal{F}_2$ and this branch satisfies $q_2 > d_x + 1 = 4$. We have that

$$\mathcal{F}_1 \equiv \mathcal{F}_2^2 \mod x^{d_x+1} \Longrightarrow (1,-2,0) \in Z$$

and we can show that this is the only possible relation. Hence $\dim Z = 1$. Since clearly $\dim S = 2$, it follows from Proposition 4.1 that $\dim V(\mathbb{Q}) = 3$. Since $s = 3$ is the dimension of the ambient space, it follows that $V(\bar{\mathbb{Q}}) = V(\mathbb{Q}) = \mathbb{Q}^3$. Observe that we could not use directly Lemma 4.3 to show this equality since F has two absolute factors $y - x + iy^5$ and $y - x + iy^5$ that are not defined over $\mathbb{Q}$.

4.3. Number of factors. Irreducibility test.

Proposition 4.4 leads to a formula for r that depends only on the M-truncated factors:

Corollary 4.6. *The number of rational factors is equal to*

$$r = \dim V(\bar{\mathbb{K}}) \cap W^{M+1} - \dim Z \cap W^{M+1},$$

hence can be computed with the only truncated precision $\max(d_x + 1, M + 1)$.

Proof. We know from Proposition 4.1 that $V(\mathbb{F}) = S \oplus Z$. Intersecting with W^n, and using that $S \subset W^n$, we get that

$$S \oplus (Z \cap W^n) = (S \oplus Z) \cap W^n = V(\mathbb{F}) \cap W^n = V(\bar{\mathbb{K}}) \cap W^n.$$

for all $n > M$, the last equality thanks to Proposition 4.4. The corollary follows by counting dimensions. □

Of course, we can not *a priori* compute M without knowing the rational factorization so that Corollary 4.6 seems to be useless from a computational point of view. However, it leads to an irreducibility test over $\mathbb{K}$ with the only $2d_x$-truncated precision.

Corollary 4.7. *The polynomial F is irreducible over $\mathbb{K}$ if and only if*

$$\dim V(\bar{\mathbb{K}}) \cap W^{2d_x} - \dim Z \cap W^{2d_x} = 1.$$

Proof. Suppose that $\dim V(\bar{\mathbb{K}}) \cap W^{2d_x} - \dim Z \cap W^{2d_x} = 1$. Since the inclusion $W^{2d_x} \subset W^n$ holds for all $n \geq 2d_x$ we deduce from Corollary 4.6 that $\dim S = 1$. Suppose now that F is irreducible over $\mathbb{K}$. Then it's enough to show that $M < 2d_x$ by the same argument. Suppose on the contrary that $M \geq 2d_x$. Since F is irreducible, we have by definition of M that $q_i \geq 2d_x$ for all i. It follows from Lemma 3.1 that

$$\mathrm{val}_x(\mathrm{Disc}_y F) = \sum_{i=1}^{s} q_i d_i \geq 2d_x \sum_{i=1}^{s} d_i = 2d_x d_y,$$

which is impossible for a degree reason. □

4.4. A combinatorial approach for solving recombinations

We show here that under some reasonable conditions, we can compute the factorization of F just by knowing $V(\mathbb{F})$ and Z, hence from the (d_x+1)-truncated analytic factors only. Let us introduce the subset

$$I := \Big\{ i \in \{1,\dots,s\},\ \ \mu \in Z \Rightarrow \mu_i = 0 \Big\}.$$

and let

$$L := \Big\{ \mu \in \mathbb{F}^s,\ \ \mu_i = 0\ \forall\, i \notin I \Big\}.$$

We denote by $\pi : \mathbb{F}^s \to L$ the natural projection on L.

Definition 4.8. We say that F is reasonably ramified over $x=0$ if

$$\dim\, \pi(V(\mathbb{F})) = \dim V(\mathbb{F}) - \dim Z.$$

In other words F is reasonably ramified if and only if for all $j=1,\dots,r$, there is an analytic factor $\mathcal{F}_i$ of F_j such that $\mu \in Z$ implies $\mu_i = 0$. In particular, if $M \leq d_x+1$, then F is reasonably ramified thanks to the proof of Proposition 4.4. Note that for fields with positive characteristic, we can test if F is reasonably ramified since we can then compute $V(\mathbb{F})$, Z and L (see Subsection 5.2). In characteristic zero, this will be the case if we know moreover that $V(\overline{\mathbb{K}}) = V(\mathbb{F})$.

Proposition 4.9. *Suppose that $\mathbb{K}$ has characteristic zero or strictly greater than d_y. Suppose that F is reasonably ramified over $x=0$. Suppose that $V(\mathbb{F}) = Z \oplus T$ for some vector subspace T whose reduced echelon basis $(w_1,\dots,w_r)$ form a partition of $(1,\dots,1)$. Then,*

$$F_j = \mathrm{prim}\left[\mathrm{lc}(F) \prod_{i=1}^{s} \mathcal{F}_i^{w_{ji}} \right]^{d_x+1} \qquad j=1,\dots,r$$

and all rational factors F_j of F can be computed within $\widetilde{O}(d_x d_y)$ field operations.

Here, prim stands for the primitive part with respect to y. In order to prove Proposition 4.9, we first need a key lemma. We denote by $R := \mathbb{K}[[x]]/(x^{d_x+1})$ and by f_i the class of $\mathcal{F}_i$ in R. Since F is not divisible by x, we have that $f_i \in R^*[y]$, where R^* stands for the multiplicative group of non zero divisors. In particular, it makes sense to compute f_i^k in the total ring of fractions of $R[y]$ for any integer $k \in \mathbb{Z}$.

Lemma 4.10. *Suppose that $\mathbb{K}$ has characteristic zero or strictly greater than d_y, and let $\mu \in \{0,1\}^s$. Then $\mu \in Z$ if and only if $\prod_{i=1}^r f_i^{\mu_i} = 1 \in R$. If $\mathbb{K}$ has characteristic zero, the same conclusion holds with the weaker hypothesis $\mu \in \mathbb{Z}^s$.*

Proof. We have equality

$$\sum \mu_i \hat{f}_i \partial_y f_i = f \frac{\left(\prod f_i^{\mu_i}\right)'}{\prod f_i^{\mu_i}}$$

in the total ring of fractions of $R[y]$. Hence $\mu \in Z$ if and only if $\left(\prod f_i^{\mu_i}\right)' = 0$, which is equivalent to that $\prod f_i^{\mu_i} \in R^*(y^p)$, where p stands for the characteristic of $\mathbb{K}$. If $p > d_y$,

and since $\mu_i \in \{0,1\}$, we necessarily have $\prod f_i^{\mu_i} \in R^*$ for a degree reason. If $p = 0$ the same holds obviously. In particular, we must have

$$\prod f_i^{\mu_i} = \prod f_i^{\mu_i}(\infty) := \prod \mathrm{lc}(f_i)^{\mu_i} = x^k,$$

for some $k \in \mathbb{Z}$. But we know that $\mathrm{val}_x(f_i) = 0$ for all i, hence we must have $k = 0$. □

Proof of Proposition 4.9. We have by assumption that $V(\mathbb{K}) = S \oplus Z$ where $\pi(Z) = 0$ and where the reduced echelon basis $(v_1, \ldots, v_s)$ of S is such that $\pi(v_1), \ldots \pi(v_s)$ are non zero vectors of $\{0,1\}^s$ in reduced echelon form. Hence the same property has to hold for the basis $(w_1, \ldots, w_s)$ of T and up to reordering the w_j's, we must have equality $\pi(w_j) = \pi(v_j)$, forcing relations $w_j - v_j \in Z$. Then the proof of Proposition 4.9 then follows from Lemma 4.10 combined with relations (2) and (3). Since w_j has entries in $\{0,1\}$, the complexity for computing F_j belongs to $\tilde{\mathcal{O}}(d_x \deg_y F_j)$ using fast multiplication in $R[y]$ (see the proof of Proposition 6.1 in Section 6 for details concerning complexity issues). The last statement then follows by adding this cost over all j. □.

Example 4.11. Let us return to example 2.2 of Subsection 2.2. We find that

$$V(\mathbb{K}) = \big\langle (1,0,0,0,1), (0,1,0,0,1), (0,0,1,1,-1) \big\rangle \quad \text{and} \quad Z = \langle (1,-1,0,0,0) \rangle.$$

It follows that $I = \{3,4,5\}$ and $L = \{\mu \in \mathbb{K}^5,\ \mu_1 = \mu_2 = 0\}$: the projection of $V(\mathbb{K})$ on L is

$$\pi(V(\mathbb{K})) = \big\langle (0,0,0,0,1), (0,0,1,1,-1) \big\rangle,$$

which has dimension $\dim V(\mathbb{K}) - \dim Z = 2 (= \dim S)$. Hence F is reasonably ramified. Let T be such that $V(\mathbb{K}) = Z \oplus T$ and such that the reduced echelon basis (w_1, w_2) of T is a partition of $(1, \ldots, 1)$. The constraints $w_i \in \{0,1\}^5 \cap V(\mathbb{K})$, $w_i \neq 0$ and $w_1 + w_2 = (1,1,1,1,1)$ lead to the two possible solutions

$$(w_1, w_2) = ((1,0,0,0,1), (0,1,1,1,0)) \quad \text{or} \quad (w_1, w_2) = ((1,0,1,1,0), (0,1,0,0,1)),$$

corresponding respectively to the factorizations

$$(F_1, F_2) = ([\mathcal{F}_1\mathcal{F}_5]^{d_x+1}, [\mathcal{F}_2\mathcal{F}_3\mathcal{F}_4]^{d_x+1}) \quad \text{or} \quad (F_1, F_2) = ([\mathcal{F}_1\mathcal{F}_3\mathcal{F}_4]^{d_x+1}, [\mathcal{F}_2\mathcal{F}_5]^{d_x+1}).$$

But we know here that $[\mathcal{F}_1]^{d_x+1} = [\mathcal{F}_2]^{d_x+1}$ since $(1,-1,0,0,0) \in Z$. Hence both solutions determine the irreducible factorization of F, as predicted by Proposition 4.9.

Example 4.12. Let us return to example 4.5. We have

$$V(\mathbb{K}) = \langle (1,0,0), (0,1,0), (0,0,1) \rangle \quad \text{and} \quad Z = \langle (1,-2,0) \rangle.$$

Here $I = \{3\}$, $L = \{\mu_1 = \mu_2 = 0\}$ and $\pi(V(\mathbb{K})) = \langle (0,0,1) \rangle$ has dimension $1 < 2 = \dim V(\mathbb{K}) - \dim Z$. So F is not reasonably ramified. The family of all possible complementary subspaces T of Z in $V(\mathbb{K})$ whose reduced echelon basis forms a partition of $(1,1,1)$ is

$$T = \langle (1,0,0), (0,1,1) \rangle, \quad T = \langle (0,1,0), (1,0,1) \rangle \quad \text{or} \quad T = \langle (0,0,1), (1,1,0) \rangle.$$

Contrary to the previous example, only the second solution leads to the good factorization of F.

Unfortunately, for more complicated examples, looking for a complementary vector space T of Z in $V(\bar{\mathbb{K}})$ whose reduced echelon basis form a partition of $(1,\dots,1)$ might not be an easy task, even though we know such a T exists. An alternative approach in the zero characteristic case is to use linear algebra over $\mathbb{Z}$. Namely, we can suppose in that case that $\mathbb{F}=\mathbb{Q}$, so that $V(\mathbb{F})\cap\mathbb{Z}^s$ is a free $\mathbb{Z}$-module or rank $\dim V(\mathbb{F})$. Recall that the Hermite normal form of a matrix with integer entries is such that the leading entry (first non zero entry) of a non-zero row is positive and strictly to the right of the leading entry of the row above it. Moreover, all entries in a column above a leading entry are non-negative and strictly smaller than the leading entry. This forces also all entries in a column below a leading entry to be zero. Such a form exists and is unique, and it conserves the row space [31]. We have:

Proposition 4.13. *Suppose that $\mathbb{K}$ has characteristic zero and that F is reasonably ramified. Then we can order the set $\{1,\dots,s\}$ such that $I=\{1,\dots,\ell\}$ for some $\ell\geq s$. Let $(w_1,\dots,w_r)$ be the first r vectors of the Hermite normal form of a basis of the free $\mathbb{Z}$-module $V(\mathbb{F})\cap\mathbb{Z}^s$. Then,*

$$F_j=\operatorname{prim}\Big[\operatorname{lc}(F)\prod_{i=1}^{s}\mathcal{F}_i^{w_{ji}}\Big]^{d_x+1}\qquad j=1,\dots,r.$$

If moreover the w_j's have positive entries, then we can compute the F_j's within $\widetilde{\mathcal{O}}(d_xd_y)$ field operations.

Proof. We have by assumption that $V(\mathbb{K})=S\oplus Z$ where $\pi(Z)=0$ and where the reduced echelon basis $(v_1,\dots,v_s)$ of S is such that $\pi(v_1),\dots,\pi(v_s)$ are non zero vectors in row echelon form. After reordering the columns as in the Proposition, it follows from the definition of the Hermite normal form that $\pi(w_j)=\pi(v_j)$, which forces $w_j-v_j\in Z\cap\mathbb{Z}^s$. The conclusion then follows from Lemma 4.10. If the w_j's have positive entries, the computation of all F_j's reduces to a product of polynomials whose total degree sum is d_y. This costs $\widetilde{\mathcal{O}}(d_xd_y)$. □

The advantage is that we reduce our recombination problem to linear algebra (over $\mathbb{Z}$). The Hermite normal form of a $n\times m$ matrix A of rank r with integer coefficients can be computed with $\widetilde{\mathcal{O}}(nmr^{\omega-1}\log(||A||))$ bit operations, where $||A||$ stands for the maximum magnitude of the entries of A [31, Chapter 6]. This *bit complexity* seems to be reasonable for our purpose although it's not clear how to compare it to the *arithmetic complexity* of the remaining steps of the algorithm. An other difficulty is illustrated in the two following examples: some of the w_j's might have negative entries, in which case the complexity of computing the F_j's may increaze.

Example 4.14. Let us continue example 4.11. After reordering, we get that the Hermite normal form of the basis of $V(\mathbb{K})\cap\mathbb{Z}^5$ is

$$\langle w_1=(1,0,1,0,1),w_2=(0,1,0,0,1),(0,0,0,1,-1)\rangle,$$

leading to the factorization

$$(F_1,F_2)=([\mathcal{F}_1\mathcal{F}_3\mathcal{F}_5]^{d_x+1},[\mathcal{F}_2\mathcal{F}_5]^{d_x+1}).$$

Here, the vectors w_1 and w_2 have positive entries, and the computation of the F_j's is fast. Note that the vectors w_1 and w_2 do not necessarily form a partition of $(1,1,1,1,1)$

any more. In particular, the analytic factor $\mathcal{F}_4$ has disappeared from the recombination process due to the relation $[\mathcal{F}_4]^{d_x+1} = [\mathcal{F}_5]^{d_x+1}$.

Example 4.15. Suppose that $s = 5$ and that

$$S = \langle (1,0,1,0,0), (0,1,0,1,1) \rangle \quad Z = \langle (0,0,1,2,-3) \rangle.$$

Then F is reasonably ramified. The Hermite normal form of the basis of $V(\mathbb{K}) \cap \mathbb{Z}^5$ is

$$\big((1,0,0,-2,3), (0,1,0,1,1), (0,0,1,2,-3)\big).$$

The vector $w_1 = (1,0,0,-2,3)$ has now negative entries and the computation of the corresponding factor

$$F_1 = \frac{f_1 f_5^3}{f_4^2}$$

is *a priori* more expensive. Note that if we had reordered the indices such that $Z = \langle (0,0,2,1,-3)$, we would have obtained w_1 and w_2 with positive entries.

Remark 4.16. In general, we can show that if F is reasonably ramified and if Z is generated by vectors with at most two non zero entries (meaning that all branches with high q-invariant intersect at most one other branch), then we necessarily have $w_j \in \mathbb{N}^s$. A concrete example for which it is not the case is given by $F = (y^6 - (y-x)^2)(y-x) \in \mathbb{Q}[x,y]$. In that case $Z = \langle (0,0,0,2,-1,-1) \rangle$.

5. Conditions for constant residues. Equations of $V(\mathbb{L})$.

There are two main approaches that allow to determine when the residues of G/F do not depend on x. The first approach is related to the first De Rham cohomology group of the complementary set of the affine curve $F = 0$ in $\mathbb{A}^2_{\mathbb{K}}$. It allows to test whether certain differential meromorphic forms are linear combinations of the logarithmic derivatives of the absolute factors of F by checking closeness. This is the approach followed by Gao [11]. The second approach, that we will follow here, is based on a divisibility criterion by F and has been developed by Lecerf [26]. Hence, this section is essentially a re-lecture of Section 1 in [26], except that we have now to take into account that the leading coefficient of F is not necessarily invertible in $\mathbb{K}[[x]]$.

From now on, we fix $\mu \in \mathbb{F}^s$ and we denote by $G := G_\mu$ the corresponding polynomial and by $\rho_1, \ldots, \rho_{d_y}$ the residues of G/F at the roots of F. We denote by $p \geq 0$ the characteristic of $\mathbb{K}$ and we adopt the convention $\mathbb{K}(x^p) = \mathbb{K}$ for $p = 0$.

5.1. Equations for $V(\bar{\mathbb{K}})$

We want to know when the residues $\rho_k \in \overline{\mathbb{K}(x)}$ lie in the subfield $\bar{\mathbb{K}}$. Since F is separable, ρ_k belongs to the separable closure $\mathbb{K}(x)^{sep} \subset \overline{\mathbb{K}(x)}$ of $\mathbb{K}(x)$. Since the usual $\bar{\mathbb{K}}$-derivation of $\bar{\mathbb{K}}(x)$ uniquely extends to a $\bar{\mathbb{K}}$-derivation of $\mathbb{K}(x)^{sep}$, we can talk about the derivative of ρ_k. Hence, an obvious necessary condition for that $\rho_k \in \bar{\mathbb{K}}$ is that its derivative vanishes. More precisely, we have the following lemma:

Lemma 5.1. *We have $\rho_k' = 0$ if and only if $\rho_k \in \overline{\mathbb{K}(x^p)}$. If moreover $\mathbb{K}$ has characteristic zero or greater than $2d_x(d_y - 1)$, then $\rho_k' = 0$ if and only if $\rho_k \in \bar{\mathbb{K}}$.*

Proof. See for instance the proof of Lemma 2.4 in [11]. □

Let us denote by $\mathbb{K}[x,y]_{m,n}$ the vector space of bivariate polynomials of degree $\leq m$ in x and $\leq n$ in y. We introduce the $\mathbb{K}$-linear operator

$$\begin{array}{rcl} \mathrm{D} : \mathbb{K}[x,y]_{d_x,d_y-1} & \longrightarrow & \mathbb{K}[x,y]_{3d_x-1,3d_y-3} \\ G & \longmapsto & \Big(G_xF_y - G_yF_x\Big)F_y - \Big(F_{xy}F_y - F_{yy}F_x\Big)G, \end{array}$$

with the standard notations F_y, F_{xy}, etc. for the partial derivatives. Let $y_k(x)$ be the root of F corresponding to the residue ρ_k. By combining the formulas

$$\rho_k(x) = \frac{G(x,y_k)}{F_y(x,y_k)} \quad \text{and} \quad y_k'(x) = -\frac{F_x(x,y_k)}{F_y(x,y_k)},$$

we are led to the equality

$$\rho_k'(x) = \frac{\mathrm{D}(G)(x,y_k)}{F_y^3(x,y_k)},$$

so that

$$\rho_k' = 0 \iff \mathrm{D}(G)(x,y_k) = 0.$$

In particular, since F is separable with respect to y, it follows that $\rho_k' = 0$ for all $k = 1,\ldots,d_y$ if and only if F divides $\mathrm{D}(G)$ in $\mathbb{K}(x)[y]$. In order to reduce this division problem to a well estimated finite number of linear equations, we localize.

Let $a \in \mathbb{K}[x]$ be an irreducible polynomial which is co-prime to the leading coefficient $\mathrm{lc}_y(F) \in \mathbb{K}[x]$ of F. We denote by

$$\mathbb{A} := \mathbb{K}[x]_{(a)}$$

the localization of $\mathbb{K}[x]$ at a. Hence, euclidean division by F in $\mathbb{A}[y]$ is well defined. Each $Q \in \mathbb{A}[y]$ has a unique a-adic expansion

$$Q(y) = \sum_{i=0}^{+\infty} q_i a^i, \qquad q_i \in \mathbb{K}[x,y],\ \deg_x q_i < \deg\, a.$$

For each pair of positive integers $0 \leq m \leq n$, we introduce the truncated polynomial

$$\big\{Q\big\}_m^n := \sum_{i=m}^{n-1} q_i a^i.$$

We have the following lemma, generalizing Lemma 3 in [26]:

Lemma 5.2. *Let F and $\mathrm{D}(G)$ as before and denote by $\mathrm{D}(G) = QF + R$ the euclidean division of $\mathrm{D}(G)$ by F in the ring $\mathbb{A}[y]$. Let*

$$m := \left\lfloor \frac{2d_x - 1}{\deg\, a} \right\rfloor + 1 \qquad \text{and} \qquad n := \left\lceil \frac{3d_x - 1}{\deg\, a} \right\rceil + 1.$$

Then F divides $\mathrm{D}(G)$ in $\mathbb{K}(x)[y]$ if and only if $\big\{Q\big\}_m^n = \big\{R\big\}^n = 0$.

Proof. Since the leading coefficient of F is invertible in $\mathbb{A}$, then F divides $\mathrm{D}(G)$ in $\mathbb{K}(x)[y]$ if and only if it divides $\mathrm{D}(G)$ in $\mathbb{A}[y]$. Suppose that F divides $\mathrm{D}(G)$ in $\mathbb{K}(x)[y]$. Since both F and $\mathrm{D}(G)$ lie in $\mathbb{K}[x,y]$ and F is primitive with respect to y, it follows from Gauss lemma that F divides $\mathrm{D}(G)$ in $\mathbb{K}[x,y]$. It follows that $R = 0$ and that $Q \in \mathbb{K}[x,y]$ has

degree $\deg_x \mathrm{D}(G) - \deg_x F \leq 2d_x - 1$. In particular, the coefficients of a^i in the a-adic expansion of Q are zeroes as soon as $i \deg a > 2d_x - 1$, that is for all $i \geq m$. In particular $\{Q\}_m^n = 0$. Conversely, suppose that $\{Q\}_m^n = \{R\}^n = 0$. Then the a-valuation of $\mathrm{D}(G) - \{Q\}^m F$ is greater or equal to n. It follows that either $\mathrm{D}(G) = \{Q\}^m F$ or

$$\deg_x(\mathrm{D}(G) - \{Q\}^m F) \geq n \deg a \geq 3d_x + a - 1.$$

But we have that

$$\deg_x \{Q\}^m \leq (m-1)\deg a + \deg a - 1 \leq 2d_x + \deg a - 2$$

so that $\deg_x(\mathrm{D}(G) - \{Q\}^m F) \leq 3d_x + \deg a - 2$. This forces equality $\mathrm{D}(G) = \{Q\}^m F$ in $\mathbb{A}[y]$. Since all members of the equality lie in $\mathbb{K}(x)[y]$, the equality holds in the ring $\mathbb{K}(x)[y]$. □

Remark 5.3. If the leading coefficient of F does not vanish at 0, then we can take $a(x) = x$ and $\mathbb{A} = \mathbb{K}[[x]]$ in the previous lemma. More generally, if $\mathbb{K}$ has cardinality greater than d_y, we can reduce to that case up to replace $F(x, y)$ by $y^{d_y} F(x, \alpha + 1/y)$ for some $\alpha \in \mathbb{K}$ such that $F(0, \alpha) \neq 0$. This Möbius transformation has a negligible cost for our purpose. It only exchanges the points $(0, \infty)$ and $(0, \alpha)$ and does not modify the geometry of F along the fiber $x = 0$.

If $\mathbb{K}$ has cardinality $\leq d_y$, then both degenerate situations $u(0) = 0$ and $F(0, \alpha) = 0$ for all $\alpha \in \mathbb{K}$ might hold simultaneously. In such a case, we need to find a prime polynomial $a \in \mathbb{K}[x]$ co-prime to u. Note that we can find such an a with $\deg a \in \mathcal{O}(\log(\deg u))$ (see the proof of Proposition 6.1 in Section 4).

Remark 5.4. The situation $a(x) \neq x$ requires to perform euclidean division in $\mathbb{A}[y]$ with $\mathbb{A} \neq \mathbb{K}[[x]]$. This may break the sparse structure of $\mathrm{D}(G)$ inherent to the sparse structure of the analytic factors $\mathcal{F}_i \in \mathbb{K}[[x]][y]$.

According to Lemma 5.2, we introduce the following $\mathbb{F}$-linear map:

$$\begin{aligned} \mathrm{D}_a : \mathbb{F}^s &\longrightarrow \mathbb{K}[x, y] \times \mathbb{K}[x, y] \\ \mu &\longmapsto \left(\frac{\{Q\}_m^n}{a^m}, \{R\}^n \right) \end{aligned}$$

where a, m, n are defined as in Lemma 5.2 and where Q and s are defined by the euclidean division $\mathrm{D}(G_\mu) = QF + R$ in $\mathbb{A}[y]$.

Corollary 5.5. *We have equality* $\ker(\mathrm{D}_a) = V(\overline{\mathbb{K}(x^p)})$. *If moreover* $\mathbb{K}$ *has characteristic zero or greater than* $2d_x(d_y - 1)$, *then* $\ker(\mathrm{D}_a) = V(\overline{\mathbb{K}})$.

Proof. Follows by combining Lemma 5.1 and Lemma 5.2. □

The image of D_a is contained in the finite-dimensional vector space

$$\mathrm{D}_a(\mathbb{F}^s) \subset \mathbb{K}[x, y]_{d_x - 1, 2d_y - 3} \times \mathbb{K}[x, y]_{3d_x - 1, d_y - 1}.$$

Hence, for $\mathbb{F} = \mathbb{K}$, the computation of $\ker(\mathrm{D}_a)$ reduces to compute the kernel of a $\mathbb{K}$-linear system of s unknowns and $\mathcal{O}(d_x d_y)$ equations.

5.2. The case of small characteristic

When the characteristic p of $\mathbb{K}$ is small, we need supplementary condition in order to know when $\rho_k \in \bar{\mathbb{K}}$. In fact, we will get in such a case the stronger conditions $\rho_k \in \mathbb{F}_p$ thanks to the following $\mathbb{F}_p$-linear operator:

$$\begin{aligned} \mathrm{N} : \mathbb{K}[x,y]_{d_x,d_y-1} &\longrightarrow \mathbb{K}[x,y^p]_{pd_x,d_y-1} \\ G &\longmapsto G^p - \partial_y^{p-1}(GF^{p-1}). \end{aligned}$$

The operator N is well defined since $\partial_y(\mathrm{N}(G)) = 0$. The vector space $\mathbb{K}[x^a,y^b]_{m,n}$ has to be understood as the vector space of polynomials of bi-degree (m,n) in the variables (x^a,y^b). The operator N was introduced by Niederreiter in the context of univariate factorization over finite fields [27], and then used for bivariate factorization in [26].

Lemma 5.6. *We have* $V(\mathbb{F}_p) = \{\mu \in \mathbb{F}_p^s \mid \mathrm{N}(G_\mu) = 0\}$

Proof. This follows from Theorem 2 in [27]. □

Since $\deg_x \mathrm{N}(G_\mu) = pd_x$, the number of linear equations to be solved for computing $\ker(\mathrm{N}(G_\mu))$ grows linearly with p. The idea developed in [26] is to combine N with the operator D in order to cut down this dependancy in p.

Lemma 5.7. *Suppose that* $\mu \in \ker(\mathrm{D}_a)$. *Then* $\mathrm{N}(G_\mu) \in \mathbb{K}[x^p,y^p]$.

Proof. See [26], Lemma 4. □

Hence, previous lemma ensures that the $\mathbb{F}_p$-linear map

$$\begin{aligned} \mathrm{N}_a : \ker(\mathrm{D}_a) &\longrightarrow \mathbb{K}[x^p,y^p]_{d_x,d_y-1} \\ \mu &\longmapsto \mathrm{N}(G_\mu) \end{aligned}$$

is well-defined. In particular, if $\mathbb{K} = \mathbb{F}_{p^k}$ is a finite field, the computation of $\ker(\mathrm{D}_a)$ reduces to compute the kernel of a $\mathbb{K}$-linear system of $\dim\ker(\mathrm{D}_a) \leq r$ unknowns and $\mathcal{O}(kd_xd_y)$ equations over $\mathbb{F}_p$.

6. Algorithms and complexity

We combine now our previous results in order to give an algorithm for factorization and an algorithm for computing the number of rational factors, and we study their complexities. We recall that we use the $\widetilde{\mathcal{O}}$ notation to hide logarithmic factors in the complexity estimates. Our cost analyses will use the following classical complexity estimates for the basic operations:

- The product of two univariate polynomials of degree at most d over a ring $\mathbb{A}$ can be be computed with $\widetilde{\mathcal{O}}(d)$ operations over $\mathbb{A}$ [16, Theorem 8.23];
- The resultant and the extended greatest common divisor of two univariate polynomials of degree at most d over a field $\mathbb{A}$ can be computed with $\widetilde{\mathcal{O}}(d)$ operations in $\mathbb{A}$ [16, Chapter 11];

- The product of s univariate polynomials $G_1, \ldots, G_s$ over a field $\mathbb{A}$ whose degree sum is d takes $\widetilde{\mathcal{O}}(d \log(s))$ operations in $\mathbb{A}$ thanks to the sub-product tree technique [16, Chapter 10];
- If $F \in \mathbb{A}[y]$ has degree d, then the remainders of F modulo all the G_i can also be computed with $\widetilde{\mathcal{O}}(d \log(s))$ operations in $\mathbb{A}$ (simultaneous reduction). The inverse problem (Chinese remaindering), has the same cost [16, Chapter 10].
- We can compute the reduced echelon basis of a vector space defined by N equations and $s \leq N$ unknowns over a field $\mathbb{A}$ with $\mathcal{O}(N s^{\omega-1})$ operations in $\mathbb{A}$, where $2 < \omega < 3$ is the usual matrix multiplication exponent [31, Theorem 2.10].

6.1. A rational factorization algorithm

We obtain finally a deterministic algorithm for irreducible rational factorization of separable bivariate polynomials. The field $\mathbb{F}$ now stands for $\mathbb{K}$ if $\mathbb{K}$ has characteristic zero or greater or equal to $d_x(d_y - 1)$ and $\mathbb{F}$ stands for the prime field $\mathbb{F}_p$ of $\mathbb{K}$ otherwise. Given a vector space V over $\mathbb{F}$, we denote by $\mathrm{reb}_{\mathbb{F}}(V)$ the reduced echelon basis of V over $\mathbb{F}$. If we say compute V, this means compute $\mathrm{reb}_{\mathbb{F}}(V)$.

Algorithm : Critical Factorization

Input: *A bivariate polynomial $F \in \mathbb{K}[x, y]$ separable with respect to y.*

Output: *The irreducible rational factors of F.*

Step 0. Compute the content $f \in \mathbb{K}[x]$ of F with respect to y and do $F \leftarrow F/f$. Compute $f_1, \ldots, f_t$ the irreducible factors of f over $\mathbb{K}$.

Step 1. Compute the truncated analytic factors $[\mathcal{F}_1]^{d_x+1}, \ldots, [\mathcal{F}_s]^{d_x+1}$ of F. If $s = 1$ then return $(f_1, \ldots, f_t, F)$. Otherwise, build the polynomials $\left[\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i\right]^{d_x+1}$ for all $i = 1, \ldots, s$ and initialize $S_0 \leftarrow \mathbb{F}^s$.

Step 2. If $\mathrm{lc}_y(F)(0) \neq 0$, let $a \leftarrow x$. Otherwise, compute $a \in \mathbb{F}[x]$ irreducible, co-prime to $\mathrm{lc}_y(F)$, of degree in $\mathcal{O}(\log d_x)$.

Step 3. Build the $\mathbb{F}$-linear system associated to D_a and compute $S_0 \leftarrow \ker(\mathrm{D}_a)$. If $\dim_{\mathbb{F}} S_0 = 1$, return $(f_1, \ldots, f_t, F)$. If $\mathbb{K}$ has characteristic zero or greater than $d_x(d_y - 1)$, then go to Step 5. Else go to Step 4.

Step 4. Build the $\mathbb{F}$-linear system associated to N_a and compute $S_0 \leftarrow S_0 \cap \ker(\mathrm{N}_a)$. If $\dim_{\mathbb{F}} S_0 = 1$, return $(f_1, \ldots, f_t, F)$. If $\mathrm{reb}(S_0)$ does not form a partition of $(1, \ldots, 1)$ or if $Z \neq 0$ then go to Step 5. Otherwise, go to Step 7.

Step 5. Compute $q := \lfloor v/d \rfloor$ where $v := \mathrm{val}_x(\mathrm{Disc}_y(F))$ and d is the minimal y-degree of the $[\mathcal{F}_i]^{d_x+1}$. If $q \leq d_x$, go to Step 7, otherwise go to Step 6.

Step 6. Compute the q-truncated analytic factors of F and compute $S_0 \leftarrow S_0 \cap W^q$.

Step 7. We have $S = S_0$. For each $v_j \in \mathrm{reb}(S)$, $j = 1, \ldots, r$, compute

$$\tilde{F}_j := \left[\mathrm{lc}(F) \prod_{i=1}^{s} \mathcal{F}_i^{v_{ji}} \right]^{d_x+1}$$

and compute the primitive part F_j of $\tilde{F}_j$ with respect to y.

Step 8. Return $(f_1, \ldots, f_t, F_1, \ldots, F_r)$.

The proof of Theorem 1 follows from the following proposition.

Proposition 6.1. *The algorithm Critical Factorization is correct. It performs at most one univariate factorisation in $\mathbb{K}[x]$ of degree d_x and :*

- If $\mathbb{K}$ has characteristic zero or greater than $d_x(d_y - 1)$, then at most

$$\mathcal{O}(d_x d_y^2 + d_y \max(d_x, q) s^{\omega-1}) + \mathcal{C}(\max(d_x, q), d_y)$$

arithmetic operations over $\mathbb{K}$.

- If $\mathbb{K} = \mathbb{F}_{p^k}$, then at most

$$\widetilde{\mathcal{O}}(k d_x d_y^2 + k d_y \max(d_x, q) s^{\omega-1}) + \mathcal{O}(k)\mathcal{C}(\max(d_x, q), d_y)$$

operations over $\mathbb{F}_p$.

Proof. We have $S_0 = V(\mathbb{F}_p)$ at the end of Step 4 by Lemma 5.1. Hence $S = S_0$ if and only if $Z = 0$ by Proposition 4.1. If $\mathrm{reb}(S_0)$ does not form a partition of $(1, \ldots, 1)$ or $Z \neq 0$, then $S \neq S_0$ and we need to go to Step 5. Otherwise, the recombination problem is solved and we can go directly to Step 7.

We have $S_0 = V(\bar{\mathbb{K}})$ or $S_0 = V(\mathbb{F})$ at the beginning of Step 5. Since $\deg_x \mathrm{lc}(\mathcal{F}_i) \leq d_x$, we have that $\deg_y \mathcal{F}_i = \deg_y [\mathcal{F}_i]^{d_x+1}$. Hence $q \geq N$ by the Remark 3.2. It follows from Theorem 3.4 and Corollary 3.5 that $S = S_0$ at Step 7. For all $j = 1, \ldots, r$, we have that $\tilde{F}_j = \frac{\mathrm{lc}(F)}{\mathrm{lc}(F_j)} F_j$ since

$$\deg_x(\mathrm{lc}(F)/\mathrm{lc}(F_j)) + \deg_x(F_j) \leq \deg_x F.$$

Hence, the algorithm returns a correct answer. Let us study its complexity.

Step 0. Computation of the content of F requires $\tilde{\mathcal{O}}(d_x d_y)$ arithmetic operations over $\mathbb{K}$.

Step 1. Computations of the $(d_x + 1)$-truncated $\mathcal{F}_i$'s has complexity $\mathcal{C}(d_x, d_y)$ by definition. Then we compute all $[\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i]^{d_x+1}$ with $\tilde{\mathcal{O}}(s d_x d_y)$ operations in $\mathbb{K}$.

Step 2. If $\mathbb{K}$ has characteristic zero or greater than d_x, we can take $a = x - c$ for some c such that $\mathrm{lc}(F)(c) \neq 0$. Otherwise, a basic approach (certainly not the most efficient) consists to remark that for $n > \log_p(\deg_x \mathrm{lc}(F))$, the polynomial

$$\tilde{a}_n := \frac{x^{p^n} - x}{\gcd(x^{p^n} - x, \mathrm{lc}(F))}$$

has positive degree and is co-prime to u. Then, we take for a an irreducible factor of $\tilde{a}_n$, which has necessary degree less or equal to $n \in \mathcal{O}(\log d_x)$. Thanks to fast gcd computations, we compute $\tilde{a}_n$ within $\tilde{\mathcal{O}}(\max(\deg_x \mathrm{lc}(F), p^n)) \subset \tilde{\mathcal{O}}(d_x)$ operations. Then, we need to perform a univariate factorization of degree at most d_x in order to find a.

Step 3. In order to build the linear system of the map D_a, we need first to compute $D_i := \mathrm{D}(G_{e_i})$ for e_i varying over the canonical basis of $\mathbb{F}^s$. This has complexity $\tilde{\mathcal{O}}(s d_x d_y)$. Then, we need to compute the a-adic expansion of the D_i's and F. This costs $\tilde{\mathcal{O}}(s d_x d_y)$ thanks to [16], Theorem 9.15. We need then to perform s euclidean divisions in $(\mathbb{A}/a^m)[y]$ of polynomials of degree $\mathcal{O}(d_y)$, and where $m \in \mathcal{O}(d_x/a)$. This costs $\tilde{\mathcal{O}}(s d_y)$ operations in $\mathbb{A}/a^m$, hence $\tilde{\mathcal{O}}(s d_x d_y)$ operations over $\mathbb{K}$. Then computing the reduced echelon basis of $\ker(\mathrm{D}_a)$ requires $\mathcal{O}(d_x d_y s^{\omega-1})$ operations in $\mathbb{K}$.

Step 4. We compute here S_0 with at most $\widetilde{\mathcal{O}}(kd_xd_ys^{\omega-1})$ arithmetic operations over $\mathbb{F}_p$ thanks to [26], Proposition 4. It has to be noticed that the construction of the linear system associated to N_a might constitute a bottleneck to the algorithm. The $\mathbb{F}$-vector space Z is determined by s unknowns and $\mathcal{O}(d_xd_y)$ equations over $\mathbb{K}$, hence testing $Z \neq 0$ requires at most $\mathcal{O}(d_xd_ys^{\omega-1})$ operations over $\mathbb{K}$. Note that $Z = 0$ as soon as F is locally irreducible along $x = 0$ (Lemma 6.5).

Step 5. Since $v \leq 2d_xd_y$, we can compute $\mathrm{Disc}_y(F)$ by considering F as a polynomial in y with coefficient in the ring $\mathbb{K}[x]/(x^{2d_xd_y})$. This requires $\widetilde{\mathcal{O}}(d_xd_y^2)$ arithmetic operations over $\mathbb{K}$ thanks to fast euclidean algorithm [16]. Computing q then has a negligible cost.

Step 6. Computing the higher truncations of the $\mathcal{F}_i$'s requires $\mathcal{C}(N, d_y)$ operations over $\mathbb{K}$ by definition. Then computing all $\left[\hat{\mathcal{F}}_i\partial_y\mathcal{F}_i\right]_{d_x+1}^{N}$ requires $\tilde{\mathcal{O}}(sNd_y)$ operations in $\mathbb{K}$. Building the linear system that determines the equations of $W^N \cap S_0$ requires at most $\tilde{\mathcal{O}}(Nd_y)$ operations in $\mathbb{K}$ thanks to the sub-product tree technique. Then computing the reduced echelon basis of $W^N \cap S_0$ requires at most $\mathcal{O}((N - d_x)d_yt^{\omega-1})$ operations over $\mathbb{K}$, where $t = \dim_{\mathbb{K}} U \leq s$.

Step 7. Let $n_j := \deg_y F_j$. Then the computation of $\tilde{F}_j$ requires $\tilde{\mathcal{O}}(d_xn_j)$ operations in $\mathbb{K}$, hence a total of $\tilde{\mathcal{O}}(d_xd_y)$ operations for all j. The cost of primitive parts computations amounts to the same number of operations.

The proof follows by adding all these costs, and by remarking that one arithmetic operation over $\mathbb{F}_{p^k}$ requires $\mathcal{O}(k)$ operations over $\mathbb{F}_p$. □

Remark 6.2. *(About Step 5.)* The cost of the discriminant computation might be very high in terms of bit complexity. Moreover, it might happen that N and q differ by a factor of the order of magnitude of d_y. Hence it is much more preferable to approximate the q_i's (hence N) during the computation of the $\mathcal{F}_i$'s, for instance by using the relations with the characteristic Puiseux exponents of the branches $\mathcal{F}_i$ (see for instance [**?**]). Hence, the cost of Step 5 is included in $\mathcal{C}(N, d_y)$. Note that if the reduced echelon basis of $V(\bar{\mathbb{K}})$ does not form a partition of $(1, \ldots, 1)$ or if $Z \neq 0$, then necessarily $N > d_x$. Finally, note that if $\mathbb{K} = \mathbb{Q}$ (or more generally a number field), there are strategies to compute the valuation of the discriminant by working modulo a well chosen prime p [**?**].

6.2. Algorithms for the number of irreducible rational factors

In the first algorithm, we suppose that $\mathbb{K}$ has positive characteristic, or that $\mathbb{K}$ is a decomposition field of F. The field $\mathbb{F}$ stands for $\mathbb{K}$ if $\mathbb{K}$ has characteristic zero or for the prime field $\mathbb{F}_p$ of $\mathbb{K}$ otherwise.

Algorithm : Number of Factors

Input: *A bivariate polynomial $F \in \mathbb{K}[x, y]$ separable with respect to y.*

Output: *The number of irreducible rational factors.*

Step 0. Compute the content $f \in \mathbb{K}[x]$ of F with respect to y and do $F \leftarrow F/f$. Compute t the number of irreducible factors of f over $\mathbb{K}$.

Step 1. Compute the $d_x + 1$-truncated analytic factors of F.

Step 2. Compute $r \leftarrow \dim V(\mathbb{F})$. If $r = 1$ then return $t + 1$.

Step 3. Compute $r \leftarrow r - \dim Z$. Return $t + r$.

Proposition 6.3. *The algorithm Number of Factors is correct. It performs at most one univariate factorisation in $\mathbb{K}[x]$ of degree d_x and :*
- If $\mathbb{K}$ has characteristic zero, then $\mathcal{O}(d_x d_y s^{\omega-1}) + \mathcal{C}(d_x, d_y)$ operations over $\mathbb{K}$.
- If $\mathbb{K} = \mathbb{F}_{p^k}$, then $\mathcal{O}(k d_x d_y s^{\omega-1}) + \mathcal{O}(k)\mathcal{C}(d_x, d_y)$ operations over $\mathbb{F}_p$.

Proof. The correctness of the algorithm follows from Proposition 4.1. In positive characteristic, we can compute $V(\mathbb{F})$ as in the previous algorithm and the complexity analysis follows from the proof of previous proposition 6.1. In characteristic zero, we have that $V(\mathbb{F}) = V(\bar{\mathbb{K}})$ by Lemma 4.3 so that we compute $V(\mathbb{F})$ as in Step 3 of algorithm Critical Factorization. The $\mathbb{F}$-vector space Z is determined by s unknowns and $\mathcal{O}(d_x d_y)$ equations over $\mathbb{K}$, hence testing $Z \neq 0$ requires at most $\mathcal{O}(d_x d_y s^{\omega-1})$ operations over $\mathbb{K}$. □

Finally, we have the following algorithm for an irreducibility test. Here, no hypothesis are made on the field $\mathbb{K}$.

Algorithm : Irreducibility Test

Input: *A bivariate polynomial $F \in \mathbb{K}[x, y]$ separable with respect to y.*

Output: *True if F is irreducible over $\mathbb{K}$, False otherwise.*

Step 0. If F is not primitive with respect to y, then return False. Otherwise, replace F by its primitive part.

Step 1. Compute the n-truncated analytic factors of F with $n = d_x + 1$ if $\mathrm{Char}(\mathbb{K}) > 0$ and $n = 2d_x$ otherwise.

Step 2. Compute $r \leftarrow \dim V(\mathbb{F})$ if $\mathrm{Char}(\mathbb{K}) > 0$ and $r \leftarrow \dim V(\bar{\mathbb{K}}) \cap W^{2dx}$ otherwise. If $r = 1$ return True.

Step 3. Compute $r \leftarrow r - \dim Z$ if $\mathrm{Char}(\mathbb{K}) > 0$ and $r \leftarrow r - \dim Z \cap W^{2d_x}$ otherwise.

Step 4. Return True if $r = 1$, False otherwise.

Proposition 6.4. *The algorithm Irreducibility Test is correct. It performs at most one univariate factorisation in $\mathbb{K}[x]$ of degree d_x and :*
- If $\mathbb{K}$ has characteristic zero, then $\mathcal{O}(d_x d_y s^{\omega-1}) + \mathcal{C}(2d_x, d_y)$ operations over $\mathbb{K}$.
- If $\mathbb{K} = \mathbb{F}_{p^k}$, then $\mathcal{O}(k d_x d_y s^{\omega-1}) + \mathcal{O}(k)\mathcal{C}(d_x, d_y)$ operations over $\mathbb{F}_p$.

Proof. The correctness of the algorithm follows from Proposition 4.1 in positive characteristic and from Proposition 4.7 otherwise. The complexity analysis follows from the proof of the two previous algorithms. □

The proof of Theorem 3 follows from the two previous propositions 6.3 and 6.4.

Let us mention that there exist also strategies based on the Newton polytope (convex hull of the support of F) that allow in some cases to detect easily the irreducibility of F [12, 14].

6.3. Locally irreducible polynomials

We recall from the introduction that we say that F is locally irreducible along the line $x = 0$ (resp. absolutely locally irreducible) if the germs of curves $(C, P) \subset (\mathbb{P}^2_{\mathbb{K}}, P)$ defined by F are irreducible over $\mathbb{K}$ (resp. over $\bar{\mathbb{K}}$) at each rational place P of the line $x = 0$, including the place at infinity.

Lemma 6.5. *Suppose that $\mathbb{K}$ has characteristic greater or equal to d_y. If F is locally irreducible along the line $x = 0$, then $Z = 0$.*

Proof. Let $\mu \in Z$. we have in particular

$$\sum_{i=1}^{s} \mu_i \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i(0, y) = 0. \tag{11}$$

Let us consider first an analytic factor $\mathcal{F}_i$ corresponding to affine place of C along $x = 0$. Since F is locally irreducible along the line $x = 0$. It follows from Hensel's lemma [16] that $\mathcal{F}_i(0, y)$ is a power of a prime polynomial that is co-prime to $\hat{\mathcal{F}}_i(0, y)$. Hence relation (11) combined with Gauss Lemma imposes that $\mathcal{F}_i(0, y)$ divides $\mu_i \partial_y \mathcal{F}_i(0, y)$, hence $\mu_i = 0$ thanks to the assumption on the characteristic of $\mathbb{K}$. Suppose now that F has an analytic factor, say $\mathcal{F}_1$ that vanishes at $(0, \infty)$. By the local irreducibility assumption, $\mathcal{F}_1$ is the unique such factor. Hence $\mu \in Z$ becomes equivalent to that

$$\mu_2 = \cdots = \mu_s = 0 \quad \text{and} \quad \mu_1 [\hat{\mathcal{F}}_1 \partial_y(\mathcal{F}_1)]^{d_x+1} = 0,$$

thanks to what we proved for the affine places. The leading coefficient of $\hat{\mathcal{F}}_1 \partial_y(\mathcal{F}_1)$ is equal to $d_1 \operatorname{lc}_y(F)$. It has degree $\leq d_x$, and $d_1 \neq 0$ by assumption on $\mathbb{K}$. Hence, last equation implies $\mu_1 = 0$. □

Lemma 6.6. *If $\operatorname{Card}(\mathbb{K}) > d_y$ and F is locally irreducible along the line $x = 0$, then we compute the $(d_x + 1)$-truncated analytic factors of F with one univariate factorization of degree at most d_y plus $\widetilde{\mathcal{O}}(d_x d_y)$ arithmetic operations over $\mathbb{K}$.*

Proof. Since $\operatorname{Card}(\mathbb{K}) > d_y$, there exists $y_0 \in \mathbb{K}$ such that $F(0, y_0) \neq 0$. To find such an element y_0 has a negligible cost once the univariate factorization of $F(0, y)$ is given. Then the Möbius transformation $F \leftarrow y^{d_y} F(x, \alpha + 1/y)$ reduce to the case where $u = \operatorname{lc}_y(F)$ is a unit modulo x. Hence we are in position where

$$F(0, y) = u(0) \prod_{i=1}^{s} P_i^{m_i}, \quad \mathcal{F}_i(0, y) = P_i^{m_i}$$

for some distinct prime polynomials $P_i \in \mathbb{K}[y]$. We can lift this factorization modulo x^{d_x+1} with $\widetilde{\mathcal{O}}(d_x d_y)$ arithmetic operations over $\mathbb{K}$ thanks to the multi-factor Hensel lifting [16], Theorem 15.18. Then, we perform the inverse Möbius transformation in order to get the analytic factors of the original polynomial. Both Möbius transformations can be done in softly optimal time $\widetilde{\mathcal{O}}(d_x d_y)$ with interpolation/evaluation. □

Proof of Theorem 2. It follows from Lemma 6.5 and Proposition 4.1 that $S = V(\mathbb{K})$ under the assumption of Theorem 2. If $\mathbb{K} = \mathbb{F}_{p^k}$ is a finite field, we can compute a basis of $V(\mathbb{K})$ from the (d_x+1)-truncated factors within $\widetilde{\mathcal{O}}(k d_x d_y s^{\omega-2})$ operations over $\mathbb{F}$ (see the proof

of Proposition 6.1). Since one operation in $\mathbb{K}$ amounts to $\mathcal{O}(k)$ operations over $\mathbb{F}$, the proof follows from Lemma 6.6. If $\mathbb{K}$ is a decomposition field for F, we have $V(\mathbb{K}) = V(\bar{\mathbb{K}})$ thanks to Lemma 4.3. Since $\mathbb{K}$ has characteristic zero or greater than $d_x(2d_y - 1)$, we compute the reduced echelon basis of $V(\bar{\mathbb{K}})$ within $\widetilde{\mathcal{O}}(d_x d_y s^{\omega-1})$ operations over $\mathbb{K}$. □

7. Absolute factorization

In order to generalize our results to the absolute case, we follow the strategy developed by Chèze-Lecerf in the regular case [9].

Absolute factorization. We denote by $E_1, \ldots, E_{\bar{r}}$ the irreducible factors of F in $\bar{\mathbb{K}}[x, y]$. We represent this factorization by a family of pairs of polynomials

$$\{(P_1, q_1), \ldots, (P_t, q_t)\}$$

where $q_k \in \mathbb{K}[z]$ is monic, $\deg_z P_k < \deg q_k$, $P_k(x, y, \phi) \in \bar{\mathbb{K}}[x, y]$ has constant bi-degree when ϕ runs over the roots of q_k, and for each factor E_i there exists a unique pair (k, ϕ) such that $q_k(\phi) = 0$ and

$$E_i(x, y) = P_k(x, y, \phi).$$

Such a representation is not unique, but is not redundant. The q_k's are irreducible if and only if the products $\prod_{q_k(\phi)=0} P_k(\phi)$ are the irreducible factors of F in $\mathbb{K}[x, y]$.

Absolute analytic factorization. We denote by $\mathcal{E}_1, \ldots, \mathcal{E}_{\bar{s}}$ the irreducible analytic factors of F in $\bar{\mathbb{K}}[[x]][y]$. As before, we suppose that the $\mathcal{E}_i$'s are given by a collection of pairs of polynomials

$$\{(\mathcal{P}_1, p_1), \ldots, (\mathcal{P}_\ell, p_\ell)\}$$

where $p_k \in \mathbb{K}[z]$ is monic, $\deg_z \mathcal{P}_k < \deg p_k$, $\mathcal{P}_k(\phi) \in \bar{\mathbb{K}}[[x]][y]$ has constant degree in y when ϕ runs over the roots of p_k, and for each $\mathcal{E}_i$ there is a unique pair (k, ϕ) such that $p_k(\phi) = 0$ and

$$\mathcal{E}_i(x, y) = \mathcal{P}_k(x, y, \phi).$$

In particular, the p_k's are separable. The p_k's are irreducible if and only if $\ell = s$, if and only if

$$(\deg_y(\mathcal{P}_k), \deg_z(p_k)) = (e_k, f_k),$$

where e_k and f_k stand for the ramification index and residual degree at the rational places of $F = 0$ over $x = 0$. We do not necessarily assume this here, the only important point from a complexity point of view being that we necessarily have

$$\bar{s} = \sum_{k=1}^{\ell} \deg_z(p_k) = \sum_{i=1}^{s} f_i.$$

In particular, the more the curve $F = 0$ is ramified over $x = 0$, the smaller the number of unknowns is. This is a great difference with the regular case, for which equality $\bar{s} = d_y$ always holds. We call the n-truncated absolute analytic factorization the data of the pairs $([\mathcal{P}_k]^{n+1}, p_k)$.

Solving recombinations with $\bar{\mathbb{K}}$-linear algebra. In analogy to the rational case, we denote by

$$\bar{S} = \langle \bar{v}_1, \ldots, \bar{v}_{\bar{r}} \rangle_{\bar{\mathbb{K}}} \subset \bar{\mathbb{K}}^{\bar{s}}$$

the $\bar{\mathbb{K}}$-vector space generated by the recombination vectors $\bar{v}_1, \ldots, \bar{v}_s$ solution to

$$E_j = \bar{u}_j \prod_{i=1}^{\bar{s}} \mathcal{E}_i^{\bar{v}_{ji}}, \quad j = 1, \ldots, \bar{r},$$

with $\bar{u}_j \in \mathbb{K}[x]$, $\bar{u}_j(0) = 1$. For $\mu \in \bar{\mathbb{K}}^{\bar{s}}$, we denote by

$$\mathcal{G}_\mu := \sum_{i=1}^{\bar{s}} \mu_i \hat{\mathcal{E}}_i \partial_y \mathcal{E}_i \in \bar{\mathbb{K}}[[x]][y].$$

We introduce the $\bar{\mathbb{K}}$-vector spaces

$$\bar{V} := \Big\{ \mu \in \bar{\mathbb{K}}^{\bar{s}} \mid [\mathcal{G}_\mu]^{d_x+1} \in \langle \hat{E}_1 \partial_y E_1, \ldots, E_{\bar{r}} \partial_y E_{\bar{r}} \rangle \Big\}.$$

Hence $\mu \in \bar{V}$ if and only if the residues of $[\mathcal{G}_\mu]^{d_x+1}/F$ lie in $\bar{\mathbb{K}}$ by Lemma 3.8. We introduce also

$$\bar{Z} := \big\{ \mu \in \bar{\mathbb{K}}^{\bar{s}} \mid [\mathcal{G}_\mu]^{d_x+1} = 0 \big\},$$

and

$$\bar{W} := \big\{ \mu \in \bar{\mathbb{K}}^{\bar{s}} \mid [\mathcal{G}_\mu]_{d_x+1}^{N} = 0 \big\}$$

where N is the separability order of F. Lemma 3.8 combined with Theorem 3.4 and Proposition 4.1 give the relations

$$\bar{S} = \bar{V} \cap \bar{W} \quad \text{and} \quad \bar{V} = \bar{S} \oplus \bar{Z}.$$

First equality leads to an algorithm for solving recombinations. The second equality leads to an algorithm for computing the number of irreducible absolute factors. The idea now is to use the Vandermonde matrices attached the polynomials p_k's in order to compute a basis of the involved vector spaces with linear algebra over $\mathbb{K}$.

The Vandermonde isomorphism. We define the partition $\{1, \ldots, \bar{s}\} = I_1 \cup \cdots \cup I_\ell$ by requiring that

$$\prod_{i \in I_k} \mathcal{E}_i(x, y) = \prod_{p_k(\phi)=0} \mathcal{P}_k(x, y, \phi), \quad k = 1, \ldots \ell.$$

These products lie in $\mathbb{K}[[x]][y]$. They coincide with the irreducible analytic factors of F if and only if the p_k's are irreducible. Let $n_k := \deg p_k$. If $\mu \in \bar{\mathbb{K}}^{\bar{s}}$, we denote by $\mu^{(k)} \in \bar{\mathbb{K}}^{n_k}$ the vector whose entries are the entries of μ whose index lie in I_k. We introduce the $\bar{\mathbb{K}}$-linear map

$$\begin{aligned} A = (A_1, \ldots, A_\ell) : \bar{\mathbb{K}}^{\bar{s}} &\longrightarrow \mathbb{K}^{\bar{s}} \otimes_{\mathbb{K}} \bar{\mathbb{K}} \\ \mu = (\mu^{(1)}, \ldots, \mu^{(\ell)}) &\longmapsto \nu := (\nu^{(1)}, \ldots, \nu^{(\ell)}) \end{aligned}$$

where A_k stands for the transposed of the Vandermonde matrix of the roots $(\phi_{k1}, \ldots, \phi_{kn_k})$ of p_k. In other words, the vector

$$\nu^{(k)} := A_k \, \mu^{(k)} \in \mathbb{K}^{n_k} \otimes \bar{\mathbb{K}}$$

is defined by

$$\nu_j^{(k)} := \sum_{i=1}^{n_k} \mu_i^{(k)} \phi_{ki}^{j-1}.$$

Since the polynomials p_k are separable, each map $A_k : \bar{\mathbb{K}}^{n_k} \to \mathbb{K}^{n_k} \otimes \bar{\mathbb{K}}$ is an isomorphism, hence so is the map A.

Recombinations over $\mathbb{K}$. For a given $\mathcal{G} \in \mathbb{K}[[x]][y,z]$, we denote by $\mathrm{coeff}(\mathcal{G}, z^j) \in \mathbb{K}[[x]][y]$ the coefficient of z^j in $\mathcal{G}$. We have by construction that $\mathcal{P}_k$ divises F in the ring $\mathbb{K}[z]/(p_k)[[x]][y]$ and we denote by $\hat{\mathcal{P}}_k$ the unique polynomial such that $F = \mathcal{P}_k\hat{\mathcal{P}}_k \in \mathbb{K}[[x]][y,z]$, with $\deg_z \hat{\mathcal{P}}_k < \deg p_k$. Given $\nu \in \bar{\mathbb{K}}^{\bar{s}}$, we denote by

$$\mathcal{H}_\nu := \sum_{k=1}^{\ell}\sum_{j=1}^{n_k} \nu_j^{(k)} \,\mathrm{coeff}(\hat{\mathcal{P}}_k\partial_y\mathcal{P}_k, z^{j-1}).$$

We introduce the $\mathbb{K}$-vector spaces

$$V_{\mathbb{K}} := \Big\{\nu \in \mathbb{K}^{\bar{s}} \mid [\mathcal{H}_\nu]^{d_x+1} \in \langle \hat{E}_1\partial_y E_1, \ldots, E_{\bar{r}}\partial_y E_{\bar{r}}\rangle_{\mathbb{K}}\Big\}$$

$$Z_{\mathbb{K}} := \Big\{\nu \in \mathbb{K}^{\bar{s}} \mid [\mathcal{H}_\nu]^{d_x+1} = 0\Big\}.$$

and

$$W_{\mathbb{K}} := \Big\{\nu \in \mathbb{K}^{\bar{s}} \mid [\mathcal{H}_\nu]_{d_x+1}^{N} = 0\Big\},$$

We have the following

Proposition 7.1. *The isomorphism $A : \mu \mapsto \nu$ induces isomorphisms*

$$\bar{V} = V_{\mathbb{K}} \otimes_{\mathbb{K}} \bar{\mathbb{K}}, \quad \bar{W} = W_{\mathbb{K}} \otimes_{\mathbb{K}} \bar{\mathbb{K}} \quad \text{and} \quad \bar{Z} = Z_{\mathbb{K}} \otimes_{\mathbb{K}} \bar{\mathbb{K}}.$$

Proof. By construction, we have that

$$\begin{aligned}
\mathcal{G}_\mu = \sum_{k=1}^{\ell}\sum_{i=1}^{n_k} \mu_i^{(k)}\hat{\mathcal{P}}_k\partial_y\mathcal{P}_k(\phi_{ki}) &= \sum_{k=1}^{\ell}\sum_{i=1}^{n_k}\sum_{j=1}^{n_k} \mathrm{coeff}(\hat{\mathcal{P}}_k\partial_y\mathcal{P}_k, z^{j-1})\phi_{ki}^{j-1} \\
&= \sum_{k=1}^{\ell}\sum_{j=1}^{n_k}\Big(\sum_{i=1}^{n_k}\phi_{ki}^{j-1}\Big)\,\mathrm{coeff}(\hat{\mathcal{P}}_k\partial_y\mathcal{P}_k, z^{j-1}) \\
&= \sum_{k=1}^{\ell}\sum_{j=1}^{n_k} \nu_j^{(k)}\,\mathrm{coeff}(\hat{\mathcal{P}}_k\partial_y\mathcal{P}_k, z^{j-1}) = \mathcal{H}_\nu.
\end{aligned}$$

The claimed isomorphisms then follow from the definitions of the involved vector spaces. □

Proof of Theorem 4. We have shown how to compute a basis of all involved vector spaces with linear algebra over $\mathbb{K}$. Unfortunately, we don't have the reduced echelon basis trick when working with the unknowns ν instead of μ. To solve this problem, we rather use an absolute partial fraction decomposition algorithm along a regular fiber, following Section 4 in [9]. We obtain the following algorithm.

Algorithm : Absolute Factorization

Input: *A field $\mathbb{K}$ with cardinality at least $d_x(2d_y-1)$ and a bivariate polynomial $F \in \mathbb{K}[x,y]$ separable with respect to y.*
Output: *A family $\{(P_1,q_1),\ldots,(P_t,q_t)\}$ that represents the absolute factorization of F.*

Step 1. Compute a basis $\nu_1, \ldots, \nu_{\bar{r}}$ of $V_{\mathbb{K}} \cap W_{\mathbb{K}}$.

Step 2. Find a regular fiber $x = \alpha$ for some $\alpha \in \mathbb{K}$.

Step 3. Compute $h_1 := \mathcal{H}_{\nu_1}(\alpha, y), \ldots, h_{\bar{r}} := \mathcal{H}_{\nu_{\bar{r}}}(\alpha, y)$.

Step 4. Call Algorithm 7 in [9] in order to find $(c_1, \ldots, c_{\bar{r}}) \in \mathbb{K}^{\bar{r}}$ that separate the residues of the h_i's.

Step 5. Let $h = \sum c_i h_i$. Call the Lazard-Rioboo-Trager algorithm (Algorithm 14 in [9]) in order to compute the absolute partial fraction decomposition of $h/F(\alpha, y)$.

Step 6. Call Algorithm 6 in [9] of absolute multi-factor Hensel lifting in order to lift the decomposition of Step 6 to $\{(P_1, q_1), \ldots, (P_t, q_t)\}$.

Proposition 7.2. *Let $m = \max(d_x + 1, N)$ and $p = \mathrm{Char}(\mathbb{K})$. The algorithm Absolute Factorization is correct. It performs at most*

$$\mathcal{O}(\bar{s}^{\omega-1} \max(d_x + 1, N) d_y + \bar{r} d_x d_y^2) + \mathcal{C}(\max(d_x + 1, N), d_y)$$

operations in $\mathbb{K}$ if $p = 0$ or $p > d_x(2d_y - 1)$ and at most

$$\widetilde{\mathcal{O}}(k\bar{s}^{\omega-1} \max(d_x + 1, N) d_y + k\bar{r} d_x d_y^2) + \mathcal{O}(k)\mathcal{C}(\max(d_x + 1, N), d_y)$$

operations over $\mathbb{F}_p$ if $\mathbb{K} = \mathbb{F}_{p^k}$.

Proof. Given the $\mathcal{P}_k$'s and the p_k's, we can compute a basis of the $\mathbb{K}$-vector spaces $V_{\mathbb{K}}$ and $W_{\mathbb{K}}$ with the the same cost as in the rational case, with the number of unknowns s being replaced by $\bar{s}$. Given $(\nu_1, \ldots, \nu_{\bar{r}})$ a basis of $V_{\mathbb{K}} \cap W_{\mathbb{K}}$, we have by construction that

$$\langle \mathcal{H}_{\nu_1}, \ldots, \mathcal{H}_{\nu_{\bar{r}}} \rangle_{\bar{\mathbb{K}}} = \langle \hat{E}_1 \partial_y E_1, \ldots \hat{E}_{\bar{r}} \partial_y E_{\bar{r}} \rangle_{\bar{\mathbb{K}}},$$

with $\mathcal{H}_{\nu_i} \in \mathbb{K}[x, y]$. By assumption on the cardinality of the field, we know that there exists a regular fiber $x = \alpha$ over which $F(\alpha, y)$ is separable of degree d_y. We can find such a fiber by computing $\mathrm{Disc}\, F(i, y)$ for $i = 1, \ldots, d_x(2d_y - 1) + 1$ until we reach a non vanishing discriminant. This costs at most $\mathcal{O}(d_x d_y^2)$ operations over $\mathbb{K}$. Then we refer to [9], Paragraph 4 for the remaining steps of the algorithm. Step 4 costs $\mathcal{O}(\bar{r} d_x d_y^2)$ operations in $\mathbb{K}$, step 5 costs $\mathcal{O}(d_y^2)$ operations in $\mathbb{K}$ and step 6 costs $\widetilde{\mathcal{O}}(d_x d_y)$ operations in $\mathbb{K}$. □

Theorem 4 follows immediately from the previous proposition.

Proof of Theorem 5. We have by Proposition 7.1 that the number of absolutely irreducible factors of F is equal to

$$\bar{r} = \dim_{\bar{\mathbb{K}}} \bar{S} = \dim_{\mathbb{K}} V_{\mathbb{K}} - \dim_{\mathbb{K}} Z_{\mathbb{K}}$$

Given the $d_x + 1$-truncated analytic factorization of F, we can compute $\dim_{\mathbb{K}} V_{\mathbb{K}}$ and $\dim_{\mathbb{K}} Z_{\mathbb{K}}$ with the same costs as in the rational case, with the number of unknowns s being replaced by $\bar{s}$. The proof of Theorem 5 follows. □

8. Non degenerate polynomials

We introduce here the P-adic Newton polytopes. These combinatorial objects give a lot of interesting informations for both rational and analytic factorization. In particular, we show here that they permit to detect a large class of polynomials whose separability order is small.

Let us fix $P \in \mathbb{K}[y]$ a non constant polynomial. Any polynomial $\mathcal{F} \in \mathbb{K}[[x]][y]$ can be uniquely expanded as

$$\mathcal{F}(x,y) = \sum f_{ij} x^i P^j \in \mathbb{K}[[x]][y],$$

with $f_{ij} \in \mathbb{K}[y]$, $\deg f_{ij} < \deg P$. Let

$$\mathrm{Supp}_P(\mathcal{F}) := \left\{(i,j) \in \mathbb{N}^2,\ f_{ij} \neq 0\right\}$$

stands for the P-support of $\mathcal{F}$. The P-adic Newton polytope of $\mathcal{F}$, or P-polytope for short, is the convex hull of the positive cone generated by the support of $\mathcal{F}$, that is

$$\mathrm{N}_{P,\mathcal{F}} := \mathrm{Conv}\left((\mathrm{Supp}_P(\mathcal{F}) + (\mathbb{R}^+)^2\right).$$

When $P = y$ we recover the usual notion of Newton polytope of a bivariate power series [21], and we might simply say Newton polytope for the y-polytope. Take care that the terminology of Newton polytope refers sometimes in the literature to the (compact) convex hull of the support of a bivariate polynomial, which also provides many interesting combinatorial restrictions on the factorization of F, see for instance [12, 13, 14, 34] and the references therein. We have the following lemma.

Lemma 8.1. *Let $P \in \mathbb{K}[y]$ be separable and irreducible and let $\alpha \in \bar{\mathbb{K}}$ be a root of P. Then, the P-polytope of $\mathcal{F}$ coincides with the Newton polytope of $\mathcal{F}(x, y+\alpha)$.*

Proof. Since P is irreducible and separable, the highest power of P that divides a given $f \in \mathbb{K}[y]$ coincides with the highest power of $y-\alpha$ that divides f in $\bar{\mathbb{K}}[y]$, which coincides with the highest power of y that divides $f(y+\alpha)$. The Lemma follows. □

We call the P-edges of $\mathcal{F}$ the compact edges of its P-polytope. Let Λ be a P-edge and let a_Λ and b_Λ stand respectively for the distance from Λ to the y-axis and x-axis. We define the P-edge polynomial of F associated to a Λ as

$$\mathrm{f}_{P,\Lambda} := x^{-a_\Lambda} y^{-b_\Lambda} \sum_{(i,j)\in\Lambda} \bar{f}_{ij} x^i y^j \in \mathbb{K}_P[x,y].$$

where $\bar{f}_{ij} \in \mathbb{K}_P := \mathbb{K}[y]/(P)$ stands for the reduction modulo P. By construction, the polynomial $\mathrm{f}_{P,\Lambda}$ is quasi-homogeneous and monic with respect to x and y. We say that a series is P-convenient if it is not divisible by P or x.

Definition 8.2. We say that $\mathcal{F} \in \bar{\mathbb{K}}[[x]][y]$ is non P-degenerate if it is P-convenient and if both P and all the P-edges polynomials of $\mathcal{F}$ are separable with respect to y. We say that $\mathcal{F}$ is non degenerate at infinity if $y^{d_y}\mathcal{F}(1/y)$ is non y-degenerate. We say that $\mathcal{F}$ is non degenerate if it is non P-degenerate for all irreducible factors P of $\mathcal{F}(0,y)$ and if it is non degenerate at infinity.

Remark 8.3. By quasi-homogeneity, we can let $x = 1$ for checking separability of the P-edge polynomials.

Remark 8.4. Usually, the notion of non degenerate polynomials in $\mathbb{K}[[x]][y]$ only allows ramification at the places $y = 0$ and $y = \infty$, while we consider here all places of $\mathbb{P}^1_{\mathbb{K}}$. A notable exception is [29] where the authors use collection of P-adic polytopes in order to improve the usual Bernstein-Koushnirenko bound for the number of solutions of a polynomial system with isolated roots.

Remark 8.5. In zero characteristic, non y-degeneracy is equivalent to the most common definition of non degeneracy introduced by Kouchnirenko [21]. In positive characteristic, there are several notion of non degeneracy. Kouchnirenko non degeneracy is equivalent to that the edge polynomials are separable with respect to x and y. This is the one that allows to generalize the Milnor formula to positive characteristic. Our notion is weaker (for instance $y^3 - x^2$ in characteristic 2). Weak non degeneracy introduced in [6], Section 3 is equivalent to that the edge polynomials are square-free. This is the one that allows to compute the number of local factors. Our notion is stronger (for instance $y^3 - x^2$ in characteristic 3).

Lemma 8.6. *Let $P \in \mathbb{K}[y]$ be separable and irreducible. Then $\mathcal{F}$ is non P-degenerate if and only if $\mathcal{F}(y + \alpha)$ is non y-degenerate at any roots α of P.*

Proof. Let α be a root of P and let us write $\mathcal{F}(y + \alpha) = \sum c_{ij} x^i y^j$ for some $c_{ij} \in \bar{\mathbb{K}}$. A straightforward computation shows that the coefficients in the two expressions are related by

$$c_{ij} = P'(\alpha)^j f_{ij}(\alpha).$$

By Lemma 8.1, the y-edges of $\mathcal{F}(y + \alpha)$ are one-to-one with the P-edges of $\mathcal{F}$. Let Λ be such an edge. The corresponding y-edge polynomial $\mathrm{f}_{y,\Lambda}$ of $\mathcal{F}(y + \alpha)$ and P-edge polynomial $\mathrm{f}_{P,\Lambda}$ of $\mathcal{F}$ are related by the formula

$$\mathrm{f}_{y,\Lambda}\left(x, \frac{y}{P'(\alpha)}\right) = x^{-a_\Lambda} y^{-b_\Lambda} \sum_{(i,j)\in\Lambda} f_{ij}(\alpha) x^i y^j = \mathrm{ev}_\alpha\left(\mathrm{f}_{P,\Lambda}\right) \in \mathbb{K}(\alpha)[x, y].$$

where ev_α is induced be the isomorphism $\mathbb{K}_P \simeq \mathbb{K}(\alpha)$ determined by α. Since the discriminant of monic polynomials commutes with specialization, we deduce that $\mathrm{f}_{y,\Lambda}$ is separable with respect to y if and only if $\mathrm{f}_{P,\Lambda}$ is. □

Proposition 8.7. *Suppose that $F \in \mathbb{K}[x, y]$ is non degenerate, then $S = V(\bar{\mathbb{K}})$.*

Proof. Let as usual $F = u\mathcal{F}_1 \cdots \mathcal{F}_s$ be the irreducible factorization of F in $\mathbb{K}[[x]][y]$. By Corollary 3.5, it's enough to prove that $q_i \leq d_x$ for all i. By point (2) in Lemma 3.1, the q-invariant of the irreducible factors of $\mathcal{F}_i$ in $\bar{\mathbb{K}}[[x]][y]$ are all equal to q_i. Hence, there is no less to suppose that $\mathbb{K} = \bar{\mathbb{K}}$. In such a case, Hensel lemma implies that we necessarily have $\mathcal{F}_i(0, y) = (y - \alpha_i)^{d_i}$ for some $\alpha_i \in \bar{\mathbb{K}}$. Since q_i is invariant under the Möbius transformations $F \leftarrow F(x, y + \alpha_i)$ (or $F \leftarrow y^{d_y} F(x, 1/y)$ for $\alpha_i = \infty$), we are reduced to estimate q_i when $\mathcal{F}_i(0, 0) = 0$. Clearly, q_i only depends on those factors $\mathcal{F}_j$ for which $\mathcal{F}_j(0, 0) = 0$ so that we can suppose that $F \in \mathbb{K}[x, y]$ is a product of Weierstrass polynomials which by Lemma 8.6 is non y-degenerate. By the multiplicative property of the resultant, we have

$$d_i q_i = \mathrm{val}_x(\mathrm{Disc}_y(\mathcal{F}_i)) + \sum_{j\neq i} \mathrm{val}_x \mathrm{Res}_y(\mathcal{F}_i, \mathcal{F}_j).$$

For given two Weierstrass polynomials $\mathcal{F}, \mathcal{G} \in \mathbb{K}[[x]][y]$, we have the formula

$$\mathrm{val}_x \, \mathrm{Res}_y(\mathcal{F}, \mathcal{G}) = (\mathcal{F}, \mathcal{G})_0$$

where $(\mathcal{F}, \mathcal{G})_0$ stands for the intersection multiplicity

$$(\mathcal{F}, \mathcal{G})_0 := \dim_{\mathbb{K}} \frac{\mathbb{K}[[x, y]]}{(\mathcal{F}, \mathcal{G})}$$

of $\mathcal{F}$ and $\mathcal{G}$ at $(0, 0)$, see for instance [32] p.28 (the proof adapts to the positive characteristic case). Let us denote by

$$\Delta_i := (\mathbb{R}^+)^2 \setminus \mathrm{N}_{\mathcal{F}_i}$$

the complementary set in $(\mathbb{R}^+)^2$ of the Newton polytope of $\mathcal{F}_i$. Note that Δ_i is compact since $\mathcal{F}_i$ is convenient by assumption. By Bernstein-Khovanskii-Kouchnirenko theorem, we have the formula

$$(\mathcal{F}_i, \mathcal{F}_j)_0 \geq [\Delta_i, \Delta_j],$$

with equality if the product $\mathcal{F}_i \mathcal{F}_j$ is non y-degenerate (the converse holds in characteristic zero). See for instance Corollary 5.6 in [8] in the case $\mathbb{K} = \mathbb{C}$ or [21] for any algebraically closed field. Here,

$$[\Delta_i, \Delta_j] := \mathrm{Vol}(\Delta_i + \Delta_j) - \mathrm{Vol}(\Delta_i) - \mathrm{Vol}(\Delta_j)$$

stands for the mixed volume of polytopes. In the same way, we have that

$$(\mathcal{F}_i, \partial_y \mathcal{F}_i)_0 \geq [\Delta_i, \Delta_i] - d_y,$$

with equality if $\mathcal{F}_i$ is non degenerate (see Theorem 5.6 in [8], the proof adapts to the positive characteristic case since f_Λ is assumed to be separable with respect to y). Since all $\mathcal{F}_i$'s are irreducible, it follows that Δ_i is a triangle with vertices $(0, 0), (a_i, 0), (0, d_i)$ where $a_i = \mathrm{val}_x(\mathcal{F}_i(x, 0))$ (with $a_i = 0$ and Δ_i being a segment if $\mathcal{F}_i$ does not depend on x). In such a case, we get that

$$[\Delta_i, \Delta_j] = \min\{d_i a_j, d_j a_i\},$$

see [8], Section 5. Hence it follows that

$$q_i d_i \leq \sum_{j=1}^{s} d_i a_j - d_y = d_i \, \mathrm{val}_x \, F(x, 0) - d_y \leq d_i d_x - d_y.$$

The inequality $q_i \leq d_x$ follows. □

Let $F \in \mathbb{K}[x, y]$ and suppose given the irreducible factorization

$$F(0, y) = \prod_{i=1}^{t} P_i^{n_i} \in \mathbb{K}[y].$$

For each i, we denote by s_i the total number of irreducible rational factors of the P_i-edges polynomials of F and by ℓ_i the lattice length of the P_i-boundary. Note the inequalities

$$s_i \leq \ell_i \leq n_i.$$

In the same way, denote by s_∞ the total number of rational irreducible factors of the edge polynomials of $y^{d_y} F(x, 1/y)$ and by ℓ_∞ the lattice length of its Newton boundary.

Lemma 8.8. *Suppose given $F \in \mathbb{K}[x,y]$ primitive with respect to y and x. Then, the respective numbers s and $\bar{s}$ of irreducible analytic factors of F over $\mathbb{K}$ and $\bar{\mathbb{K}}$ satisfy*

$$s \leq s_F := \sum_{i=1}^{t} s_i + s_\infty \quad \text{and} \quad \bar{s} \leq \bar{s}_F := \sum_{i=1}^{t} \ell_i \deg P_i + \ell_\infty,$$

both inequality being equalities if F is non degenerate along the fiber $x = 0$.

Proof. Suppose first F monic w.r.t y. By Hensel's Lemma, the number of irreducible factors of F in $\mathbb{K}[[x]][y]$ is the sum of the numbers of irreducible factors in the local rings $\mathbb{K}[[x]][y]_{(P_i)}$ when P_i runs over the irreducible factors of $F(0,y)$. Then the assertion for s follows for instance from Chapter 6 in [7]. For the absolute case, we consider the decomposition

$$\bar{\mathbb{K}}[[x]][y]_{(P_i)} = \bigoplus_{P(\alpha)=0} \bar{\mathbb{K}}[[x, y-\alpha]].$$

By Lemma 4.10 in [6], the number of absolute factors of F in $\bar{\mathbb{K}}[[x]][y]_{(y-\alpha)}$ is bounded by the lattice length of the Newton boundary of $F(x, y+\alpha)$, which by Lemma 8.1 coincides with ℓ_i. Moreover, there is equality if $F(x, y+\alpha)$ is non y-degenerate, which is the case when F is non degenerate by Lemma 8.6. Summing up over all the roots of P_i and over all i, we get the result. If F is not monic, we conclude in the same way by taking also into account the place at infinity. □

Remark 8.9. Equalities $s = s_F$ and $\bar{s} = \bar{s}_F$ hold in fact with the weaker hypothesis that the edge polynomials are square-free.

Example 8.10. Suppose that

$$F(x,y) = y(y^2-2)^3 - x^2(y^2-2) + x^5 \in \mathbb{Q}[x,y].$$

Then $F(0,y) = y(y^2-2)^2$ has two irreducible coprime factors $P_1 = y$ and $P_2 = y^2 - 2$. There is a unique P_1-edge polynomial $\mathrm{f}_{\Lambda,P_1} = -8y + 2x^2$, which is obviously separable and irreducible. Hence $s_1 = \ell_1 = 1$. There are two P_2-edge polynomials

$$\mathrm{f}_1 := \phi y^2 - x^2 \quad \text{and} \quad \mathrm{f}_2 := -y + x^3$$

where $\phi \in \mathbb{Q}_{P_2}$ stands for the residue class of y. Both polynomials are separable. Since ϕ is not a square, f_1 is irreducible over $\mathbb{Q}_{P_2}$, but has two factors over $\bar{\mathbb{Q}}$. Obviously, f_2 has exactly 1 factor over any field. Hence $s_2 = 1 + 1 = 2$ while $\ell_2 = 2 + 1 = 3$. Since there are no points at infinity, we finally get that F has exactly $s = s_1 + s_2 = 3$ irreducible factors in $\mathbb{Q}[[x]][y]$ and $\bar{s} = \ell_1 + 2\ell_2 = 7$ irreducible factors in $\bar{\mathbb{Q}}[[x]][y]$.

Example 8.11. Suppose that

$$F(x,y) = y^6(y^2+1)^{15} - x^{10}(1+y^{21}) \in \mathbb{K}[x,y],$$

where $\mathbb{K}$ is any field of characteristic $p \neq 2$. Then

$$F(0,y) = y^6(y^2+1)^{15}$$

has only two distinct irreducible factors $P_1 = y$ and $P_2 = y^2 + 1$. There is a unique P_1-edge polynomial $\mathrm{f}_{\Lambda,P_1} = y^6 - x^{10}$. It is separable with respect to y if and only if $p \neq 2, 3$, and we have $s_1 = \ell_1 = 2$ if $p \neq 2$. There is a unique P_2-edge polynomial

$$\mathrm{f}_{\Lambda,P_2} = \phi^6 y^{15} - x^{10}(1+\phi^{21}) = -y^{15} + (1+\phi)x^{10},$$

where ϕ stands for the residue class of y in $\mathbb{K}_{P_2} = \mathbb{K}[y]/(y^2+1)$. This polynomial is separable if and only if $p \neq 2, 3, 5$ and it is square-free if and only if $p \neq 2$. For $p \neq 2, 3, 5$, it has $s_2 = 2$ irreducible factors over $\mathbb{K}_{P_2}$ while the lattice length of Λ is $\ell_2 = 5$. Hence, if $p \neq 2, 3, 5$, then F is non degenerate and has $s = s_1 + s_2 = 4$ factors in $\mathbb{K}[[x]][y]$ and $\bar{s} = \ell_1 + 2\ell_2 = 12$ factors in $\bar{\mathbb{K}}[[x]][y]$.

Corollary 8.12. *There is a deterministic algorithm that, given $F \in \mathbb{K}[x, y]$, returns False if F is degenerate and returns the irreducible factors of F over $\mathbb{K}$ otherwise. The cost of this algorithm is one univariate factorization of degree at most d_y and*

$$\mathcal{O}(d_x d_y s_F^{\omega-1}) + \mathcal{C}(d_x, d_y)$$

operations over $\mathbb{K}$ if $p > d_x(2d_y - 1)$ or

$$\mathcal{O}(k d_x d_y s_F^{\omega-1}) + \mathcal{O}(k)\mathcal{C}(d_x, d_y)$$

operations over $\mathbb{F}_p$ if $\mathbb{K} = \mathbb{F}_{p^k}$.

Proof. The algorithm is as follows. We first compute the factorization $F(0, y) = \prod_{i=1}^{t} P_i^{n_i}$. For each i, we test the separability of P_i and of all the P_i-edges polynomials of F. This step costs at most $\mathcal{O}(d_x d_y)$ operations over $\mathbb{K}$. If F is non degenerate along the fiber $x = 0$, then $s = s_F$ by Lemma 8.8 and the separability order satisfies $N \leq d_x$ by Proposition 8.7. Hence we can take $q = d_x$ in Theorem 1. Corollary 8.12 follows. □

Remark 8.13. Analytic factorization of non degenerate polynomials may be reduced to Newton iteration in the rings $\mathbb{K}_P[[x]][y]$ after some translations and monomial change of coordinates. A first estimate leads in that case to $\mathcal{C}(d_x, d_y) \subset \mathcal{O}(s_F d_x d_y^2)$, but we believe we can do better. One of the main obstruction is the difficulty to use a dichotomic multi-factor Hensel lifting as in the regular case.

Remark 8.14. A cheap pretreatment of F is to look at the fibers $x = 0$ and $x = \infty$ (or $y = 0$ and $y = \infty$ by reversing the roles played by x and y) in order to check if there is a fiber over which F is non degenerate and with the smallest s_F or $\bar{s}_F$ as possible. If we take for instance $F(x, y) = y^6(y-1)^{15} - x^{10} + x^9 y^{21}$, then the fiber $x = 0$ leads to $s_F = 4$ and $\bar{s}_F = 7$ while the fiber $x = \infty$ would lead to $s = \bar{s} = 1$ from which we immediately deduce that F is absolutely irreducible, whatever the field is. This kind of strategies based on the relations between the (global) Newton polytope and bivariate factorization have already been considered in the literature, see for instance [12, 13, 14, 34] and the references therein.

9. Conclusion

When compared to the regular case, a great advantage of working along a critical fiber for factorization is that one has in general less analytic factors to recombine (always strictly less in the absolute case $\mathbb{K} = \bar{\mathbb{K}}$). Unfortunately, this might require in general a higher truncated precision, and our main Theorem 3 seems to suggest a bad worst case complexity. However, the important classes of non degenerate polynomials and locally irreducible polynomials illustrate that we sometimes gain in complexity when compared to the regular case. Might this hold in all generality ? We discuss briefly the two main obstructions for this.

9.1. *Fast analytic factorization ?*

The strength of our approach deeply relies on the complexity of N-truncated analytic factorization. This is a crucial problem in singularity theory. One approach in characteristic zero or $> d_y$ is to compute the rational Puiseux series. There are well known algorithms for this. Thanks to the recent paper [28], this can be done with complexity $\mathcal{O}(d^4)$ in terms of the total degree d of F in the case of finite fields. This has to be compared to the complexity of absolute factorization. In order to fit also in the rational factorization complexity class, we would need $\mathcal{O}(d^{\omega+1})$ for analytic factorization. This is an open problem.

Note that there exists algorithms for testing local analytic irreducibility of a germ of curve that do not require the use of Puiseux series. The main ingredient is that of *approximate roots* and uses essentially resultants computations [1], [23], [10]. Up to our knowledge, no complexity analysis have been done yet.

In characteristic $p < d_y$, the concept of Puiseux series does not make sense and analytic factorization is a much more delicate problem. See for instance [19] for the generalization of Puiseux series in small positive characteristic.

9.2. *Fast recombinations ?*

Even if we get a fast algorithm for computing the N-truncated analytic factors, our brute force analysis of the recombination problem in this paper led to a complexity $\mathcal{O}(Nd_y r^{\omega-2}) \subset \mathcal{O}(d^{\omega+2})$. However, the polynomials $\left[\hat{\mathcal{F}}_i \partial_y \mathcal{F}_i\right]^{N+1}$ we want to recombine have a very particular structure. Namely, they vanish with very high order at some points of the curve $F = 0$. An approach could be to write these polynomials in a basis constituted of adjoint polynomials. The number of required equations for solving recombinations (divisibility test by F or closeness of differential forms) would then decrease. This fact is illustrated in some of our previous works, where we studied the relations between resolution of singularities and factorization [35] or toric geometry and factorization [34]. Namely we developed factorization algorithms whose linear algebra steps belongs to $\mathcal{O}(p_a s^{\omega-1})$, with $p_a \leq d^2$ being the arithmetic genus of the strict transform of the curve $F = 0$ after some sequences of blowing-ups.

References

[1] Abhyankar S.S., *Irreducibility criterion for germs of analytic functions of two complex variables*, Advances in Math. 74 (1989), 190-257.

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

[3] Bernardin B., Monagan M., *Efficient Multivariate Factorization Over Finite Fields*, Proceedings of AAECC '97, LNCS 1255 (1997), 15-28.

[4] Bernstein D.N., *The number of roots of a system of equations*, Funct. Anal. Appl. 9, no. 3 (1975), 183-185.

[5] Bostan A., Lecerf G., Salvy B., Schost E., Wiebelt B., *Complexity issues in bivariate polynomial factorization*, Proceedings of ISSAC'04 (2004), 42-49.

[6] Boubakri Y., Greuel G.-M., Markwig T., *Invariants of hypersurface singularities in positive characteristic*, Revista Mat. Complutense 25 (2012), 61-85.

[7] Cassels J.W.S., *Local Fields*, London Math. Society Student Texts no.3 (1986).

[8] Cassou-Nogues P., Ploski A., *Invariants of plane curve singularities and Newton diagrams*, Univ. Iagel. Acta Math. (2011) 9-34.
[9] Chèze G. and Lecerf G., *Lifting and recombination techniques for absolute factorization*, J. of Complexity 23, no. 3 (2007), 380-420.
[10] Cossart V., Moreno-Socas G., *Irreducibility criterion: a geometric point of view*, Valuation theory and its applications II, Fields Inst. Commun., 33, Amer. Math. Soc., Providence, RI (2003) 27-42.
[11] Gao S., *Factoring multivariate polynomials via partial differential equations*, Math. Comp. 72 (2003), 801-822.
[12] Gao, S., *Absolute Irreducibility of Polynomials via Newton polytopes*, Journal of Algebra 237, Issue 2 (2001), 501-520.
[13] Gao S., Lauder A.G.B., *Decomposition of polytopes and polynomials*, Discrete Comput. Geom. 26 (2001), 89-104.
[14] Gao S., Rodrigues V. M., *Irreducibility of polynomials modulo p via Newton Polytopes*, J. Number Theory 101 (2003), 32-47.
[15] Gathen J., *Irreducibility of multivariate polynomials*, Journal of Computer and System Sciences 31 (1985), 225-264.
[16] Gathen J., Gerhard J., *Modern computer algebra*, second ed., Cambridge University Press, Cambridge, MA, (2003).
[17] Kaltofen E., *Polynomial factorization 1982-1986*, Lect. Notes in Pure and Applied Math. 125 (1990), 285-309.
[18] Kaltofen E., *Polynomial factorization 1987-1991*, Lect. Notes Comput. Sci. 583 (1992), 294-313.
[19] Kedlaya K., *The algebraic closure of the power series field in positive characteristic.* Proc. Amer. Math. Soc. 129, no. 12 (2001), 3461-3470.
[20] Khovanski A.G., *The index of polynomial vector field* (Russian), Funkt. Anal. Prloz. 13, no. 1 (1979), 49-58.
[21] Kouchnirenko A.G., *Polyèdres de Newton et nombres de Milnor*, Inventiones math. 32 (1976), 1-31.
[22] Kouchnirenko A.G., *Newton polytopes and the Bezout theorem*, Functional analysis and its applications (1976), 233-235.
[23] Kuo T. C., *Generalized Newton-Puiseux theory and Hensel's lemma in* $\mathbb{C}[[x, y]]$, Canad. J. Math. 41 (1989), 1101-1116.
[24] Lecerf G., *Sharp precision in Hensel lifting for bivariate polynomial factorization*, Math. Comp. 75 (2006), 921-933,
[25] Lecerf G., *Fast separable factorization and applications*, Applicable Algebra in Engineering, Communication and Computing 19, no.2 (2008), 135-160.
[26] Lecerf G., *New recombination algorithms for bivariate polynomial factorization based on Hensel lifting*, Applicable Algebra in Engineering, Communication and Computing 21, no.2 (2010), 151-176.
[27] Niederreiter H., *Factorization of polynomials and some linear-algebra problems over finite fields*, Linear Algebra Appl. 192 (1993), 301-328.
[28] Poteaux A., Rybowicz M., *Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields*, Proceedings of ISSAC'15 (2015), 299-306.
[29] Philippon P., Sombra M., *A refinement of the Bernstein-Kushnirenko estimate*, Advances in Mathematics 218 (2008), 1370-1418.

[30] Stadelmeyer P., Winkler F., *Computing the System of Adjoint Plane Curves by Puiseux Expansion*, Tech. report 97-38 RISC Report Series, Univ. Linz, Austria (1997).
[31] Storjohann A., *Algorithms for matrix canonical forms*, PhD thesis, TEH, Zürich (2000), http://www.scg.uwaterloo.ca/~astorjoh.
[32] Teissier B., *Introduction to curve singularities*, Singularity theory (Trieste, 1991), World Scientific Publishing (1995), 866-893.
[33] Wall C.T.C, *Singular points of plane curves*, London Math. Society (2004).
[34] Weimann M., *A lifting and recombination algorithm for rational factorization of sparse polynomials*, J. of Complexity 26, no 6 (2010), 608-628.
[35] Weimann M., *Factoring bivariate polynomials using adjoints*, J. of Symb. Comp. 58 (2013), 77-98.