EFFICIENT ALGORITHMS FOR COMPUTING RATIONAL FIRST INTEGRALS AND DARBOUX POLYNOMIALS OF PLANAR POLYNOMIAL VECTOR FIELDS

ALIN BOSTAN, GUILLAUME CHÈZE, THOMAS CLUZEAU,
AND JACQUES-ARTHUR WEIL

Abstract. We present fast algorithms for computing rational first integrals with bounded degree of a planar polynomial vector field. Our approach is inspired by an idea of Ferragut and Giacomini ([FG10]). We improve upon their work by proving that rational first integrals can be computed via systems of linear equations instead of systems of quadratic equations. The main ingredients of our algorithms are the calculation of a power series solution of a first order differential equation and the reconstruction of a bivariate polynomial annihilating a power series. This leads to a probabilistic algorithm with arithmetic complexity $\tilde{\mathcal{O}}(N^{2\omega})$ and to a deterministic algorithm solving the problem in $\tilde{\mathcal{O}}(d^2N^{2\omega+1})$ arithmetic operations, where N denotes the given bound for the degree of the rational first integral, and where $d \leq N$ is the degree of the vector field, and ω the exponent of linear algebra. We also provide a fast heuristic variant which computes a rational first integral, or fails, in $\tilde{\mathcal{O}}(N^{\omega+2})$ arithmetic operations. By comparison, the best previous algorithm given in [Chè11] uses at least $d^{\omega+1}\,N^{4\omega+4}$ arithmetic operations. We then show how to apply a similar method to the computation of Darboux polynomials. The algorithms are implemented in a Maple package RationalFirstIntegrals which is available to interested readers with examples showing its efficiency.

1. Introduction

Context. Let $\mathbb{K}$ denote an effective field of characteristic zero, i.e, one can perform arithmetic operations and test equality of two elements (typically, $\mathbb{K} = \mathbb{Q}$ or $\mathbb{Q}(\alpha)$, where α is an algebraic number). Given two polynomials A, B in $\mathbb{K}[x, y]$, we consider the planar polynomial vector field

$$\text{(S)} \qquad \left\{ \begin{array}{rcl} \dot{x} & = & A(x,y), \\ \dot{y} & = & B(x,y), \end{array} \right.$$

and discuss the problem of computing rational first integrals of (S), i.e., rational functions $F \in \mathbb{K}(x, y) \setminus \mathbb{K}$ that are constant along the solutions $(x(t), y(t))$ of (S). More precisely, the present article is concerned with the following algorithmic problem:

($\mathcal{P}_N$): given a degree bound $N \in \mathbb{N}$, either compute a rational first integral $F \in \mathbb{K}(x, y) \setminus \mathbb{K}$ of (S) of total degree at most N, or prove that no such F exists.

This old problem was already studied by Darboux in 1878 ([Dar78]) and has been the subject of numerous works ever since. The naive approach (by indeterminate

Date: October 10, 2013.

coefficients) leads to a polynomial system of quadratic equations in the coefficients of F. Other methods use what is called nowadays *Darboux polynomials*, in the spirit of the celebrated Prelle-Singer's method [PS83]; see Subsection 2.3 for a review. These methods also require solving a polynomial system of quadratic equations. Recently, Chèze [Chè11] has shown that problem $(\mathcal{P}_N)$ can be solved in polynomial time in N. The importance of this result is mainly theoretical since the exponent in the polynomial complexity estimate is bigger than 10.

To improve upon this current state of affairs, our starting point is the article [FG10] of Ferragut and Giacomini. The key observation is that (S) has a rational first integral if and only if all power series solutions in $\mathbb{K}[[x]]$ of the first order non-linear differential equation

$$\frac{dy}{dx} = \frac{B(x,y)}{A(x,y)} \tag{E}$$

are *algebraic* over $\mathbb{K}(x)$. Furthermore, minimal polynomials of these algebraic power series lead to rational first integrals.

The algorithm in [FG10] still involves solving a polynomial system of quadratic equations. Indeed, the key observation above is merely used to reduce the number of equations in the quadratic system provided by the naive approach.

Our main contributions. In the present article, we push further the observation of Ferragut and Giacomini, so as to give fast algorithms solving Problem $(\mathcal{P}_N)$. In particular, we prove that this can be done by considering only systems of *linear* equations instead of systems of quadratic equations.

We design a probabilistic algorithm that uses $\tilde{\mathcal{O}}(N^{2\omega})$ arithmetic operations in $\mathbb{K}$, where $\omega \in [2,3]$ is the exponent of linear algebra over $\mathbb{K}$, and the soft-O notation $\tilde{\mathcal{O}}(\,)$ indicates that polylogarithmic factors are neglected. The probabilistic algorithm is then turned into a deterministic one, that solves Problem $(\mathcal{P}_N)$ in arithmetic complexity $\tilde{\mathcal{O}}(d^2\, N^{2\omega+1})$, where $d = \max(\deg(A), \deg(B))$ denotes the degree of the polynomial vector field (S). This compares well to the previous polynomial time algorithm given in [Chè11], which uses at least $d^{\omega+1}N^{4\omega+4}$ arithmetic operations. Note that if we take $\omega = 3$ (i.e., the cost of naive linear algebra), then the above means that the best previously known complexity would be in $\tilde{\mathcal{O}}(d^4N^{16})$ whereas our deterministic algorithm would use at most $\tilde{\mathcal{O}}(d^2N^7)$ arithmetic operations, and our probabilistic one would use $\tilde{\mathcal{O}}(N^6)$. Lastly, we sketch a heuristic method that uses $\tilde{\mathcal{O}}(N^{\omega+2})$ arithmetic operations (i.e., $\tilde{\mathcal{O}}(N^5)$ using classical linear algebra) which is sub-cubic, given that the output has size $\mathcal{O}(N^2)$.

We provide algorithmic details, notably precise degree bounds and complexity estimates. The algorithms developed in the article are implemented in a Maple package called RationalFirstIntegrals which is available with various examples at http://www.ensil.unilim.fr/~cluzeau/RationalFirstIntegrals.html. Using this implementation, we demonstrate the efficiency of our algorithms on some examples. Finally, we show how to apply a similar method to the computation of Darboux polynomials.

Structure of the article. In Section 2, we recall Darboux's approach to the integrability of polynomial vector fields, related works, and existing results about the problem $(\mathcal{P}_N)$. We also give useful facts on the so-called *spectrum problem*. We recall in Section 3 the connection between rational first integrals of the polynomial

vector field (S) and algebraic power series solutions of (E). We then propose a first algorithm, based on linear algebra, that solves Problem ($\mathcal{P}_N$). Building on this, we develop in Section 4 an efficient probabilistic algorithm, and then turn it into an efficient deterministic algorithm. In Section 5, we study the arithmetic complexity of the algorithms developed in Section 4, and discuss several algorithmic issues. Then, in Section 6 we present our implementation and display its behavior on various examples. Finally, Section 7 shows how similar ideas can be used for computing the set of all irreducible Darboux polynomials (of a given degree) of planar polynomial vector fields.

Notation. The degree $\deg(P)$ of a bivariate polynomial $P \in \mathbb{K}[x,y]$ is the total degree of P. A rational function P/Q with $P, Q \in \mathbb{K}[x,y]$ is said to be *reduced* when P and Q are coprime. The degree $\deg(F)$ of a reduced rational function $F = P/Q$ is the maximum of $\deg(P)$ and $\deg(Q)$.
We denote by $\overline{\mathbb{K}}$ an algebraic closure of the field $\mathbb{K}$.
We write $\dot{f} := \frac{\partial f}{\partial t}$ for the usual formal derivative of the "function" (polynomial, or power series) f with respect to the variable t.
For a set Ω, we denote by $|\Omega|$ its cardinality.

2. Review on first integrals of polynomial vector fields

In this section, we recall several useful facts, mainly to keep the exposition as self-contained as possible, and to clarify the understanding of the algorithms that we develop below. Some results are not original.

2.1. First definitions and classical results.

We consider an autonomous planar polynomial vector field

$$\text{(S)} \qquad \begin{cases} \dot{x} &= A(x,y), \\ \dot{y} &= B(x,y), \end{cases}$$

where x and y are unknown "functions" of the time variable t, A and B are polynomials in $\mathbb{K}[x,y]$, and $d := \max(\deg(A), \deg(B))$ denotes the degree of the polynomial vector field. Without any loss of generality, A and B will be assumed to be coprime in the remaining of the article.

To (S) is attached the *derivation*

$$\mathcal{D} := A(x,y)\,\frac{\partial}{\partial x} + B(x,y)\,\frac{\partial}{\partial y},$$

acting on the polynomial ring $\mathbb{K}[x,y]$. We thus view $\mathbb{K}[x,y]$ as a differential ring endowed with the derivation $\mathcal{D}$. We denote by $\mathbb{K}(x,y)$ its field of fractions.

Definition 1. A *rational first integral of* (S) is a non-constant rational function $F \in \mathbb{K}(x,y) \setminus \mathbb{K}$ satisfying $\mathcal{D}(F) = 0$.

A rational first integral F of (S) is thus a non-trivial constant for the derivation $\mathcal{D}$. Intuitively, this means that if $(x(t), y(t))$ is a pair of "functions" satisfying (S), then $F(x(t), y(t))$ is constant when t varies. We explain in Theorem 11 below why no algebraic extension of the base field is necessary in Definition 1.

A starting observation is that the rational function $F = P/Q$ is a first integral for (S) if and only if $\mathcal{D}(P)\,Q = \mathcal{D}(Q)\,P$. Therefore, if F is a *reduced* rational first integral for (S), then P divides $\mathcal{D}(P)$, and Q divides $\mathcal{D}(Q)$ in $\mathbb{K}[x,y]$. This motivates the following definition.

Definition 2. A polynomial $M \in \overline{\mathbb{K}}[x,y] \setminus \overline{\mathbb{K}}$ is a *Darboux polynomial for* $\mathcal{D}$ if M divides $\mathcal{D}(M)$ in $\overline{\mathbb{K}}[x,y]$. Therefore, if M is a Darboux polynomial for $\mathcal{D}$, then there exists a polynomial $\Lambda \in \overline{\mathbb{K}}[x,y]$ such that $\mathcal{D}(M) = \Lambda M$. Such a polynomial $\Lambda \in \overline{\mathbb{K}}[x,y]$ is called a *cofactor associated with the Darboux polynomial* M.

Darboux polynomials were introduced by G. Darboux in [Dar78]. These polynomials correspond to algebraic curves invariant under the vector field. The following lemma will be used in the sequel: it means that if we have a non-singular initial condition, then there is a unique irreducible invariant algebraic curve satisfying this initial condition, see [Sin92, Lemma A.1].

Lemma 3. *Let* $\mathcal{D} = A(x,y)\frac{\partial}{\partial x} + B(x,y)\frac{\partial}{\partial y}$ *be the derivation attached to* (S) *and let* (x_0,y_0) *be a non-singular point of* $\mathcal{D}$*, i.e.,* $A(x_0,y_0) \neq 0$ *or* $B(x_0,y_0) \neq 0$*. If* M_1 *and* M_2 *are two Darboux polynomials for* $\mathcal{D}$ *such that* $M_1(x_0,y_0) = M_2(x_0,y_0) = 0$ *and if* M_1 *is irreducible, then* M_1 *divides* M_2*.*

Darboux polynomials are sometimes called *partial first integrals* in the literature. The reason is that rational first integrals and Darboux polynomials are intimately related notions: as sketched above, numerators and denominators of reduced rational first integrals are Darboux polynomials. The converse is also true, see Corollary 5 below.

A fundamental property of Darboux polynomials is given in the following lemma (see, e.g., [DLA06, Lemma 8.3, p. 216]) that can be proved by a straightforward calculation.

Lemma 4. *Let* $M \in \overline{\mathbb{K}}[x,y]$ *and let* $M = M_1\,M_2$ *be a factorization of* M *in* $\overline{\mathbb{K}}[x,y]$*, with* M_1 *and* M_2 *coprime. Then,* M *is a Darboux polynomial for* $\mathcal{D}$ *if and only if* M_1 *and* M_2 *are Darboux polynomials for* $\mathcal{D}$*. Furthermore, if* Λ_M*,* Λ_{M_1} *and* Λ_{M_2} *denote respectively the cofactors of* M*,* M_1 *and* M_2*, then* $\Lambda_M = \Lambda_{M_1} + \Lambda_{M_2}$*.*

As a corollary we get:

Corollary 5. *Let* $F = P/Q$ *be a reduced rational function in* $\mathbb{K}(x,y)$*. Then* F *is a rational first integral of* (S) *if and only if* P *and* Q *are Darboux polynomials for* $\mathcal{D}$ *with the same cofactor.*

The previous corollary gives a relation between Darboux polynomials and rational first integrals. The next theorem shows that if we have enough Darboux polynomials, then we have a rational first integral, see [Sin92, Appendix] for a modern proof.

Theorem 6. *[Darboux-Jouanolou* [Dar78, Jou79, Sin92]*]*
If $d = \max(\deg(A), \deg(B))$*, then the polynomial vector field* (S) *has a reduced rational first integral* P/Q *if and only if* $\mathcal{D}$ *has at least* $d\,(d+1)/2 + 2$ *irreducible Darboux polynomials. In this case,* $\mathcal{D}$ *has infinitely many irreducible Darboux polynomials and any of them divides a linear combination* $\lambda\,P - \mu\,Q$*, for some* λ*,* $\mu \in \overline{\mathbb{K}}$ *not both zero. Moreover, all but finitely many irreducible Darboux polynomials are of the form* $\lambda\,P - \mu\,Q$ *and have the same degree.*

A useful corollary of Theorem 6 is the following, see [Sin92]:

Corollary 7. *For each planar polynomial vector field* (S)*, there exists a non-negative integer* $N_{(S)}$ *such that any* irreducible *Darboux polynomial for the derivation* $\mathcal{D}$ *attached to* (S) *has degree at most* $N_{(S)}$*.*

Given a derivation $\mathcal{D}$, the problem of finding a bound for the degree of irreducible Darboux polynomials is known to be difficult: this is the so-called *Poincaré problem*. It has been deeply studied in the literature and many partial results exist ([Poi91, CLN91, Car94, Per02, Wal00, CG06, LY05] and others) though the question is not fully solved yet. The fact that the derivation $\mathcal{D} = n\,x\,\frac{\partial}{\partial x} + y\,\frac{\partial}{\partial y}$ with $n \in \mathbb{N}^*$ admits $x - y^n$ as an irreducible Darboux polynomial shows that a bound depending only on the degrees of the entries cannot exist: arithmetic conditions on the coefficients of $\mathcal{D}$ have to be taken into account as well.

Consequently, given a planar polynomial vector field (S), or equivalently a derivation $\mathcal{D}$, two distinct problems occur when we want to compute rational first integrals:

(1) Find a bound on the degree of the numerator and denominator of a rational first integral, that is a bound on the degree of irreducible Darboux polynomials;
(2) $(\mathcal{P}_N)$: given a degree bound $N \in \mathbb{N}$, either compute a rational first integral $F \in \mathbb{K}(x,y) \setminus \mathbb{K}$ of (S) of total degree at most N, or prove that no such F exists.

Our aim is to give an efficient algorithm to handle the second problem $(\mathcal{P}_N)$.

In this article we suppose that $d \leq N$. This hypothesis is natural because if a derivation has a polynomial first integral of degree N, then we can show that $d \leq N - 1$, see [FL07, Theorem 6] or [Poi91].

2.2. **Non-composite rational functions and their spectrum.** We recall here the definition of *composite* rational functions and what is called the *spectrum* of a rational function. We then use these notions to describe the kernel of the derivation $\mathcal{D}$ and to give some of its properties.

Definition 8. A rational function $F(x,y) \in \mathbb{K}(x,y)$ is *composite* if it can be written $F = u \circ h$, i.e., $F = u(h)$, where $h \in \mathbb{K}(x,y) \setminus \mathbb{K}$ and $u \in \mathbb{K}(T)$ with $\deg(u) \geq 2$. Otherwise F is said to be *non-composite*.

In [MO04, Chè12b], the authors propose different algorithms for the decomposition of rational functions using properties of Darboux polynomials and rational first integrals of the Jacobian derivation.

Lemma 9. *The set of all rational first integrals of* (S) *is a* $\mathbb{K}$*-algebra. It is closed under composition with rational functions in* $\mathbb{K}(T)$*, and moreover,* F *is a rational first integral of* (S) *if and only if* $u \circ F$ *is a rational first integral of* (S) *for some* $u \in \mathbb{K}(T) \setminus \mathbb{K}$.

Proof. The first assertion directly follows from the fact that the derivation $\mathcal{D} = A(x,y)\,\frac{\partial}{\partial x} + B(x,y)\,\frac{\partial}{\partial y}$ is $\mathbb{K}$-linear and satisfies Leibniz's rule

$$\mathcal{D}(F_1 F_2) = F_1\,\mathcal{D}(F_2) + \mathcal{D}(F_1)\,F_2.$$

The second assertion follows from the equality

$$\mathcal{D}(u \circ F) = u'(F)\,\mathcal{D}(F),$$

and the fact that $u'(F)$ is zero if and only if $u \in \mathbb{K}$. □

A more precise version of Lemma 9 is given by the next theorem which completely describes the $\mathbb{K}$-algebra structure of the set of all rational first integrals of (S). This theorem seems to be a folklore result but we have not found a suitable reference. Consequently, a complete proof is provided here.

Theorem 10. *Let $\mathcal{D}$ be the derivation attached with (S). Then we have:*

$$\{G \in \mathbb{K}(x,y) \mid \mathcal{D}(G) = 0\} = \mathbb{K}(F),$$

for some non-composite reduced rational first integral F of (S).
Then any other rational first integral G of (S) is of the form $G = u \circ F$ for some $u \in \mathbb{K}(T) \setminus \mathbb{K}$. In particular, any two non-composite reduced rational first integrals are equal, up to a homography.

Proof. Let $\mathbb{L} = \{G \in \mathbb{K}(x,y) \mid \mathcal{D}(G) = 0\}$. We have $\mathbb{K} \subset \mathbb{L} \subset \mathbb{K}(x,y)$, so, from [Sch00, Theorem 1, p. 12], we deduce that $\mathbb{L}$ is finitely generated over $\mathbb{K}$ and that $\mathbb{L} = \mathbb{K}(f_1, f_2, f_3)$ for some $f_1,\ f_2,\ f_3 \in \mathbb{K}(x,y)$.
As for $i \in \{1,2,3\}$, $A(x,y)\,\frac{\partial f_i}{\partial x} + B(x,y)\,\frac{\partial f_i}{\partial y} = 0$, we get that:

$$\frac{\partial f_i}{\partial y}\frac{\partial f_j}{\partial x} - \frac{\partial f_i}{\partial x}\frac{\partial f_j}{\partial y} = 0, \quad \text{for all } i,\ j \in \{1,2,3\}.$$

The Jacobian criterion implies that f_1, f_2, f_3 are algebraically dependent and thus the transcendence degree of $\mathbb{L}$ over $\mathbb{K}$ is equal to one. By the extended Luroth's theorem, see [Sch00, Theorem 3, p. 15], we get $\mathbb{L} = \mathbb{K}(F)$, for $F \in \mathbb{K}(x,y)$. In particular, F is a rational first integral of (S).
Now, if F is composite, $F = u(H)$, with $\deg(u) \geq 2$, then $\mathbb{K}(F) \subsetneq \mathbb{K}(H)$, see, e.g., [GRS02, Proposition 2.2]. By Lemma 9, H is also a rational first integral of (S) so that $H \in \mathbb{L}$ and $\mathbb{K}(H) \subset \mathbb{L}$. This yields $\mathbb{L} = \mathbb{K}(F) \subsetneq \mathbb{K}(H) \subset \mathbb{L}$, which is absurd. Thus F is non-composite which gives the desired result. □

As a consequence of Theorem 10, *non-composite reduced* rational first integrals coincide with rational first integrals with minimal degree; they will play a key role in the remaining of this text.

In Definition 1, we have defined rational first integrals as elements of $\mathbb{K}(x,y)$. The next theorem explains why it is in general not necessary to consider rational first integrals in $\overline{\mathbb{K}}(x,y)$. To our knowledge this result is proved here for the first time. In [MM97], the authors show that if there exists a rational first integral in $\overline{\mathbb{K}}(x,y)$, then there also exists a rational first integral in $\mathbb{K}(x,y)$. We improve this result by taking into account the degrees of these rational first integrals.

Theorem 11. *If (S) admits a non-composite rational first integral in $\overline{\mathbb{K}}(x,y)$, then it admits a non-composite rational first integral in $\mathbb{K}(x,y)$ with the same degree.*

Proof. Let $f \in \overline{\mathbb{K}}(x,y)$ be a non-composite rational first integral of (S). We denote by $N(f)$ the product

$$N(f) = \prod_{\sigma_i \in G} \sigma_i(f),$$

where G is the Galois group over $\mathbb{K}$ of the smallest Galois extension containing all the coefficients of f, and we have $N(f) \in \mathbb{K}(x,y)$. As $A, B \in \mathbb{K}(x,y)$, $N(f)$ is also a rational first integral of (S). Thus, by Lemma 9, there exists a non-composite rational first integral $F \in \mathbb{K}(x,y)$ of (S). Now, applying Theorem 10 with

ground field $\overline{\mathbb{K}}$ instead of $\mathbb{K}$, we get that $F = u(f)$, with $u \in \overline{\mathbb{K}}(T)$. Furthermore, by [BCN11, Theorem 13], F is non-composite in $\mathbb{K}(x, y)$ implies that F is non-composite in $\overline{\mathbb{K}}(x, y)$. It thus follows that $\deg(u) = 1$ so that $\deg(F) = \deg(f)$. □

Now, we introduce the *spectrum* of a rational function which will play a crucial role in our algorithms.

Definition 12. Let $P/Q \in \mathbb{K}(x, y)$ be a reduced rational function of degree N. The set

$$\sigma(P, Q) = \{(\lambda : \mu) \in \mathbb{P}^1_{\overline{\mathbb{K}}} \quad | \quad \lambda P - \mu Q \text{ is reducible in } \overline{\mathbb{K}}[x, y], \text{ or } \deg(\lambda P - \mu Q) < N\}$$

is called the *spectrum* of P/Q.

In the context of rational first integrals of polynomial vector fields, the elements of the spectrum are sometimes called *remarkable values*, see, e.g., [FL07]. There exists a vast bibliography about the spectrum, see for example [Rup86, Lor93, Vis93b, Vis93a, AHS03, Bod08, BC11].

The spectrum $\sigma(P, Q)$ is finite if and only if P/Q is non-composite and if and only if the pencil of algebraic curves $\lambda P - \mu Q = 0$ has an irreducible general element, see for instance [Jou79, Chapitre 2, Théorème 3.4.6] or [Bod08, Theorem 2.2] for detailed proofs.

To the authors' knowledge, the first effective result on the spectrum is due to Poincaré. In [Poi91], he establishes a relation between the number of *saddle points* and the cardinal of the associated spectrum, in the case where all the singular points of the polynomial vector field are distinct. In particular this yields the bound $|\sigma(P, Q)| \leq d^2$ on the cardinality of the spectrum. This bound was improved recently in [Chè12a]:

Theorem 13. *Let $\mathcal{D}$ be the derivation attached with (S) and d denotes the degree of (S). If P/Q is a reduced non-composite rational first integral of (S), then:*

$$|\sigma(P, Q)| \leq \mathcal{B}(d) + 1, \text{ where } \mathcal{B}(d) = \frac{d(d+1)}{2}.$$

As a consequence of Theorem 13 and Corollary 5, if P/Q is a reduced non-composite rational first integral of (S), then for all but $\mathcal{B}(d) + 1$ constants $\sigma \in \overline{\mathbb{K}}$, the polynomial $P - \sigma Q$ has degree N and is an irreducible Darboux polynomial for $\mathcal{D}$ with the same cofactor as P and Q. This means that if (S) has a rational first integral, there exist an infinite number of irreducible Darboux polynomials which all have the same degree (and the same cofactor).

The following lemma will be useful in Section 4 for the study of our probabilistic and deterministic algorithms.

Lemma 14. *If $P/Q \in \mathbb{K}(x, y)$ is a reduced non-composite rational function of degree at most N, then the number of values of $c \in \overline{\mathbb{K}}$ for which $(Q(0, c) : P(0, c))$ belongs to $\sigma(P, Q)$ is bounded by $N\,(\mathcal{B}(d) + 1)$.*

Proof. Let $c \in \overline{\mathbb{K}}$ be such that $(Q(0, c) : P(0, c)) \in \sigma(P, Q)$. By Theorem 13, $\sigma(P, Q)$ contains at most $\mathcal{B}(d) + 1$ elements. Now, for each $(\lambda : \mu) \in \sigma(P, Q)$, as P and Q are of degree at most N, there exist at most N values of c such that $\lambda Q(0, c) - \mu P(0, c) = 0$. This ends the proof. □

2.3. **Existing algorithms for computing rational first integrals and Darboux polynomials of bounded degree.** There is a vast literature regarding the computation of rational or elementary first integrals (see for example [FG10, MM97, Chè11, PS83, SGR90, Sin92, LZ10, DDdMS01, Poi91]) and Darboux polynomials (see for example [CMS09, CMS06, CGG05, Wei95, Dar78]). Note that, among these articles, very few restrict to the specific question of rational first integrals. Surveys on computing first integrals (not restricted to planar systems) can be found for example in [Gor01, Sch93, DLA06] and [Olv93] for symmetry methods which we do not address here.

Given a degree bound N, the *naive* approach to solve $(\mathcal{P}_N)$ consists in using the method of undetermined coefficients. This leads to a system of polynomial (quadratic) equations in the unknown coefficients of the rational first integral, see [Chè11] for a complexity estimate of this approach.

Interest in Darboux polynomials has been revived by the appearance of the Prelle-Singer's method, [PS83, MM97, DDdMS01]. In [CMS06, CMS09], Coutinho and Menasché Schechter give necessary conditions for the existence of Darboux polynomials. Other necessary conditions are contained in [CGGL03, CGG05] and also in works on inverse integrating factors [CGGL03, CFL10]. The bottleneck of the Prelle-Singer's method and all of its variants is the computation *by undetermined coefficients* of all irreducible Darboux polynomials of bounded degree, which leads again to solving a polynomial system. This yields an exponential complexity algorithm, see [Chè11].

In [Chè11], Chèze shows that if the derivation $\mathcal{D}$ admits only finitely many irreducible Darboux polynomials of degree at most N, then it is possible to compute all of them by using the so-called *ecstatic curve* introduced in [Per01] within a number of *binary operations* that is *polynomial* in the bound N, in the degree $d = \max(\deg(A), \deg(B))$ of $\mathcal{D}$ and in the logarithm of the height of A and B. A nontrivial modification of this algorithm provides a polynomial-time method to solve $(\mathcal{P}_N)$, see again [Chè11]. To our knowledge, this is the first algorithm solving $(\mathcal{P}_N)$ in polynomial-time. Unfortunately, the exponent is quite large, making the algorithm unpractical even for moderate values of N. This drawback is due to the fact that algorithm Rat-First-Int in [Chè11] needs to compute the irreducible factors of a bivariate polynomial of degree $\approx dN^4$, and the best known algorithms for solving this subtask have arithmetic complexity, e.g., $\tilde{\mathcal{O}}(d^{\omega+1}N^{4\omega+4})$, see [BLS+04, Lec06].

Last, we mention the article [FG10] of Ferragut and Giacomini, where the algebraicity of a generic power series solution of the differential equation (E) is used to improve the efficiency of the naive algorithm. Precisely, the system of quadratic equations yielding the coefficients of a rational first integral is reduced to a simpler system of (still quadratic) equations. Although this gives a good heuristic improvement on the naive method, we show in the present article how to turn it into a fast algorithm. Starting from the link between (S) and (E), we reduce $(\mathcal{P}_N)$ to solving a system of *linear* equations. Furthermore, we give tight bound on the number of terms of power series solutions of (E) that are sufficient to detect the existence of rational first integrals and to compute one of them when it exists. This enables us

to turn the heuristic in [FG10] into an algorithm with polynomial complexity, that is more efficient both in theory and in practice than all previous algorithms, see Section 6.

3. Rational first integrals, differential equations and algebraic power series

3.1. Algebraic power series and rational first integrals.

Definition 15. A formal power series $y(x) \in \mathbb{K}[[x]]$ is said to be *algebraic* if it is algebraic over $\mathbb{K}(x)$, that is, if there exists a non-zero polynomial $M \in \mathbb{K}[x, y]$ such that $M(x, y(x)) = 0$. An irreducible polynomial $M \in \mathbb{K}[x, y]$ satisfying $M(x, y(x)) = 0$ is called a *minimal polynomial of* $y(x)$ in $\mathbb{K}[x, y]$.

With the planar polynomial vector field (S), we associate the first order non-linear differential equation:

$$\frac{dy}{dx} = \frac{B(x, y)}{A(x, y)} \tag{E}$$

We may assume without any loss of generality that x does not divide A, i.e., $A(0, y) \not\equiv 0$. We will explain how we can reduce to this situation and study the complexity of this reduction in Subsection 5.1.

Then, the formal version of the Cauchy-Lipschitz theorem for non-linear (first-order) differential equations ensures that for any $c \in \mathbb{K}$ such that $A(0, c) \neq 0$, the equation (E) admits a unique power series solution $y_c(x) \in \mathbb{K}[[x]]$ satisfying $y_c(0) = c$. Note that high-order truncations of the power series $y_c(x)$ can be computed efficiently using the algorithm of Brent and Kung [BK78].

The following standard result is fundamental to both our method and the one of Ferragut and Giacomini in [FG10].

Proposition 16. *Consider the planar polynomial vector field (S) and assume that $A(0, y) \not\equiv 0$. Let $c \in \mathbb{K}$ satisfy $A(0, c) \neq 0$ and $y_c(x) \in \mathbb{K}[[x]]$ be the unique power series solution of (E) such that $y_c(0) = c$.*

1. *If (S) admits a non-composite rational first integral P/Q, then the power series $y_c(x)$ is algebraic. More precisely, $y_c(x)$ is a root of the non-zero polynomial $\lambda P - \mu Q$, where $\lambda = Q(0, c)$ and $\mu = P(0, c)$.*
2. *If P/Q is a reduced non-composite rational first integral of (S) of degree at most N, then, for all but at most $N(\mathcal{B}(d) + 1)$ values of $c \in \mathbb{K}$, the polynomial $\lambda P - \mu Q$, where $\lambda = Q(0, c)$ and $\mu = P(0, c)$ is a minimal polynomial of $y_c(x)$.*

Proof. Let $F = P/Q$ be a non-composite rational first integral of (S). Since the spectrum $\sigma(P, Q)$ is finite, we can suppose that P and Q are irreducible and coprime. Let us first show that $P(0, c) \neq 0$ or $Q(0, c) \neq 0$. As $(0, c)$ is a non-singular point of $\mathcal{D}$, if $P(0, c) = Q(0, c) = 0$, then Lemma 3 implies that $P = \alpha Q$ with $\alpha \in \mathbb{K}$. As P and Q are coprime, we get a contradiction so that necessarily $P(0, c) \neq 0$ or $Q(0, c) \neq 0$.
We thus suppose $Q(0, c) \neq 0$ else we consider the rational first integral Q/P instead

of P/Q. As $Q(0,c) \neq 0$, the power series $Q(x, y_c(x))$ is invertible so that $\mathcal{D}(F) = 0$ yields $\mathcal{D}(F)(x, y_c(x)) = 0$. The latter equality can be written

$$A(x, y_c(x))\, \frac{\partial F}{\partial x}(x, y_c(x)) + B(x, y_c(x))\, \frac{\partial F}{\partial y}(x, y_c(x)) \quad = \quad 0.$$

Dividing the equality by the invertible power series $A(x, y_c(x))$ and using the fact that $y_c(x)$ is a solution of (E), we obtain

$$\begin{aligned} \frac{\partial F}{\partial x}(x, y_c(x)) + \frac{B(x, y_c(x))}{A(x, y_c(x))}\, \frac{\partial F}{\partial y}(x, y_c(x)) &= 0, \\ \frac{\partial F}{\partial x}(x, y_c(x)) + \frac{dy_c(x)}{dx}\, \frac{\partial F}{\partial y}(x, y_c(x)) &= 0, \\ \frac{d\big(F(x, y_c(x))\big)}{dx} &= 0. \end{aligned}$$

It follows that $F(x, y_c(x)) = \sigma_c$, for some $\sigma_c \in \mathbb{K}$. Consequently, we have

$$P(x, y_c(x)) - \sigma_c\, Q(x, y_c(x)) = 0,$$

with $\sigma_c = P(0,c)/Q(0,c)$ which proves (1).
If, in addition, $F = P/Q$ is reduced non-composite of degree at most N, then (2) follows directly from Lemma 14. □

Proposition 16 shows in particular that if (S) has a rational first integral P/Q, then all power series solutions of (E) are algebraic. The next proposition which is well known (see [FG10, Wei95]) asserts that the converse is also true.

Proposition 17. *Let (S) be a planar polynomial vector field, $\mathcal{D}$ the associated derivation, and (E) be the associated differential equation.*

1. *If $M \in \mathbb{K}[x,y]$ is an irreducible Darboux polynomial for $\mathcal{D}$, then all roots $y(x) \in \overline{\mathbb{K}(x)}$ of M such that $A(0, y(0)) \neq 0$ are power series solutions of (E).*
2. *The minimal polynomial of an algebraic solution $y(x) \in \mathbb{K}[[x]]$ of (E) such that $A(0, y(0)) \neq 0$ is a Darboux polynomial for $\mathcal{D}$.*
3. *(S) admits a rational first integral if and only if all the power series solutions of (E) are algebraic.*

Proof. Assume first that $M \in \mathbb{K}[x,y]$ is an irreducible Darboux polynomial for $\mathcal{D}$, and that $y(x) \in \overline{\mathbb{K}(x)}$ is a root of M, i.e., $M(x, y(x)) = 0$. Since M divides $\mathcal{D}(M)$, it follows that $y(x)$ is also a root of $\mathcal{D}(M)$. This implies

$$\frac{\partial M}{\partial x}(x, y(x)) = -\frac{B(x, y(x))}{A(x, y(x))}\, \frac{\partial M}{\partial y}(x, y(x)).$$

On the other hand, $M(x, y(x)) = 0$ implies by differentiation with respect to x that

$$\frac{\partial M}{\partial x}(x, y(x)) = -\frac{dy(x)}{dx}\, \frac{\partial M}{\partial y}(x, y(x)).$$

These two equalities provides

$$\frac{\partial M}{\partial y}(x, y(x)) \left(\frac{dy(x)}{dx} - \frac{B(x, y(x))}{A(x, y(x))} \right) = 0.$$

As M is irreducible, $\dfrac{\partial M}{\partial y}(x, y(x)) \neq 0$ so that $y(x)$ is a solution of (E). As mentioned before $A(0, y(0)) \neq 0$ implies $y(x) \in \mathbb{K}[[x]]$ (Cauchy-Lipschitz theorem) which proves (1).

Assume now that $y(x) \in \mathbb{K}[[x]]$ is an algebraic solution of (E) such that $A(0, y(0)) \neq 0$, and let M be its minimal polynomial. Then

$$0 = \frac{d\big(M(x, y(x))\big)}{dx} = \frac{\partial M}{\partial x}(x, y(x)) + \frac{dy(x)}{dx}\,\frac{\partial M}{\partial y}(x, y(x)),$$

and since $y(x)$ is a solution of (E), the latter equality implies that $y(x)$ is also a root of $\mathcal{D}(M)$. Now as M is the minimal polynomial of $y(x)$, it follows that M divides $\mathcal{D}(M)$, i.e., M is a Darboux polynomial for $\mathcal{D}$ and we have proved (2).

Let us now prove (3). If all the power series solutions of (E) are algebraic, then by (2), $\mathcal{D}$ admits infinitely many Darboux polynomials. Then Theorem 6 shows that (S) admits a rational first integral. The proof ends here since the other implication of (3) has been proved in Proposition 16. □

3.2. **Algebraic power series solutions of (E).** We have seen in Proposition 16 that if P/Q is a reduced non-composite rational first integral of (S), then a minimal polynomial of a power series solution of (E) is generically of the form $\lambda P - \mu Q$ for some constants λ and μ. Thus, if we are able to compute such a minimal polynomial, we can deduce the rational first integral P/Q. In practice, we do not compute a power series $y_c(x) \in \mathbb{K}[[x]]$ solution of (E) but only a truncation of $y_c(x)$, i.e., a finite number of terms of its expansion on the monomial basis. Given a degree bound N for the rational first integral that we are searching for, the following lemma shows that computing $y_c(x) \mod x^{N^2+1}$, i.e., the first N^2+1 terms of its expansion, is enough for our purposes.

Such an analysis of the needed precision for the power series solutions of (E) that we compute is not included in [FG10]. Note that this kind of strategy was already used in a polynomial factorization setting (see, e.g., [Kal85]) and in a differential equations setting (see [ACFG05, BCS+07]). The next lemma is a small improvement of [ACFG05, Lemma 2.4].

Lemma 18. *Let $\mathbb{L}$ be a field of characteristic 0 such that $\mathbb{K} \subseteq \mathbb{L}$. Let $\hat{y}(x) \in \mathbb{L}[[x]]$ denote an algebraic power series whose minimal polynomial $M \in \mathbb{L}[x, y]$ has degree at most N. If $\tilde{M} \in \mathbb{L}[x, y]$ is a polynomial of degree at most N satisfying*

$$(\star): \ \tilde{M}(x, \hat{y}(x)) \equiv 0 \mod x^{N^2+1},$$

then $\tilde{M}(x, \hat{y}(x)) = 0$. Moreover, if $\tilde{M}$ has minimal degree in y among polynomials satisfying $(\star)$, then $\tilde{M} = f\,M$ for some $f \in \mathbb{L}[x]$.

Proof. By definition, M satisfies $(\star)$ so there exists $\tilde{M} \in \mathbb{L}[x, y]$ of degree at most N satisfying $(\star)$. Let $\tilde{M}$ be such a solution of $(\star)$ and consider

$$\mathcal{R}(x) := \mathrm{Res}_y(M(x, y), \tilde{M}(x, y)),$$

the resultant of M and $\tilde{M}$ with respect to y. As there exist polynomials S and T in $\mathbb{K}[x, y]$ such that $S\,M + T\,\tilde{M} = \mathcal{R}$, Relation $(\star)$ yields $\mathcal{R}(x) \equiv 0 \mod x^{N^2+1}$. By Bézout's theorem, we have $\deg(\mathcal{R}) \leq \deg(M)\,\deg(\tilde{M}) \leq N^2$, thus $\mathcal{R} = 0$. This implies that M and $\tilde{M}$ have a non-trivial common factor. Now, as M is irreducible, necessarily M divides $\tilde{M}$ and thus $\tilde{M}(x, \hat{y}(x)) = 0$. Finally, if $\tilde{M}$ is supposed to

have minimal degree in y among polynomials satisfying $(\star)$, we have necessarily $\tilde{M} = f\,M$ for some $f \in \mathbb{L}[x]$ which ends the proof. □

Note that in $(\star)$, the power series $\hat{y}(x)$ can be replaced by its truncation $\hat{y}(x) \bmod x^{N^2+1}$.

Remark 19. For a given power series $\hat{y}(x)$, computing all the polynomials $\tilde{M}$ of degree at most N satisfying $(\star)$ can be done by taking an ansatz for $\tilde{M}$ and performing linear algebra calculations (e.g., solving a system of linear equations). Consequently, computing "all" solutions of $(\star)$ means computing "a basis" of solutions of the linear algebra problem associated with $(\star)$. An efficient method to address this problem and to get, via a row-echelon form, a solution of $(\star)$ with minimal degree in y is given in Subsection 5.3 where a complexity analysis is provided.

In the sequel, we say that $\tilde{M}$ is a *minimal solution of* $(\star)$ if it is a solution of $(\star)$ with minimal degree in y.

3.3. **A first algorithm for computing rational first integrals.** We now propose a first algorithm, based on linear algebra, for solving $(\mathcal{P}_N)$. More efficient algorithms, based on this one, are given in Section 4. The strategy of this algorithm is then used in Section 7 for computing Darboux polynomials.

Algorithm GenericRationalFirstIntegral

`Input:` $A, B \in \mathbb{K}[x,y]$ s.t. $A(0,y) \not\equiv 0$ and a bound $N \in \mathbb{N}$.
`Output:` A non-composite rational first integral of (S) of degree at most N, or "None".

(1) For an indeterminate c, compute the polynomial $y_c \in \mathbb{K}(c)[x]$ of degree at most (N^2+1) s.t. $y_c(0) = c$ and $\frac{dy_c}{dx} \equiv \frac{B(x,y_c)}{A(x,y_c)} \bmod x^{N^2+1}$.

(2) Compute all[1] non-trivial polynomials $\tilde{M} \in \mathbb{K}(c)[x,y]$ of degree $\leq N$ s.t.

$$(\star) : \tilde{M}(c, x, y_c(x)) \equiv 0 \mod x^{N^2+1}.$$

If no such $\tilde{M}$ exists, then Return "None". Else, among the solutions of $(\star)$, pick a *minimal* solution $\overline{M} \in \mathbb{K}[c][x,y]$.

(3) Let M denote the primitive part of $\overline{M}$ relatively to y.
Set $P(x,y) := M(0,x,y)$.
Pick any $c_1 \in \mathbb{K}$ s.t. $\frac{M(c_1,x,y)}{P(x,y)} \notin \mathbb{K}$ and set $Q(x,y) := M(c_1,x,y)$.

(4) If $\mathcal{D}(P/Q) = 0$, then Return P/Q. Else Return "None".

In the above algorithm, the output "None" means that there is no rational first integral of degree at most N but it may exist a rational first integral of degree strictly greater than N.

[1] i.e., a basis over $\mathbb{K}(c)$, see Remark 19.

Theorem 20. *Algorithm* GenericRationalFirstIntegral *is correct: either it finds a non-composite rational first integral of* (S) *of degree at most N if it exists, or it proves that no such rational first integral exists.*

To prove Theorem 20, we shall need the following lemma.

Lemma 21. *Consider the planar polynomial vector field* (S) *and assume that $A(0,y) \not\equiv 0$. If F is a reduced rational first integral of* (S)*, then $F(0,y) \in \mathbb{K}(y) \setminus \mathbb{K}$.*

Proof. Let $F = P/Q$ be a reduced rational first integral of (S). Proceeding by contradiction, we assume $F(0,y) = c_0 \in \mathbb{K}$. Then $P(0,y) - c_0\,Q(0,y) = 0$ so that x divides $P(x,y) - c_0\,Q(x,y)$. Now, from Corollary 5, $P(x,y) - c_0\,Q(x,y)$ is a Darboux polynomial for $\mathcal{D}$ and thus, by Lemma 4, x is also a Darboux polynomial for $\mathcal{D}$. Consequently, we get that x divides $A(x,y)$ and thus $A(0,y) = 0$. This is absurd so we conclude $F(0,y) \in \mathbb{K}(y) \setminus \mathbb{K}$. □

Proof of Theorem 20. Suppose first that there exists a rational first integral of (S) of degree at most N. Then, without loss of generality, we can consider a reduced non-composite one P_0/Q_0, see Lemma 9. Let $y_c \in \mathbb{K}(c)[[x]]$ be the power series solution of (E) satisfying $y_c(0) = c$. By Proposition 16, y_c is a root of $\lambda\,P_0 - \mu\,Q_0$, where $\lambda = Q_0(0,c)$ and $\mu = P_0(0,c)$. As P_0/Q_0 is non-composite, it follows that $\lambda\,P_0 - \mu\,Q_0$ is irreducible in $\mathbb{K}(c)[x,y]$. Indeed, by Lemma 21, the constant μ/λ belongs to $\mathbb{K}(c) \setminus \mathbb{K}$ and thus, from Lemma 14, we can find $c_0 \in \mathbb{K}$ such that $(Q_0(0,c_0) : P_0(0,c_0)) \notin \sigma(P_0,Q_0)$. Consequently $\lambda\,P_0 - \mu\,Q_0$ is a minimal polynomial of y_c. In Step (1), we compute the first N^2+1 terms of y_c. Now, in Step (2), if there exists a solution $\tilde{M} \in \mathbb{K}(c)[x,y]$ of $(\star)$ of degree at most N, then, Lemma 18 applied with $\mathbb{L} = \mathbb{K}(c)$ implies that $\overline{M} = f\,(\lambda\,P_0 - \mu\,Q_0)$ with $f \in \mathbb{K}(c)[x]$, where $\overline{M} \in \mathbb{K}[c][x,y]$ is defined in Step (2). Therefore, taking the primitive part of $\overline{M}$ with respect to y, in Step (3), we have $M = g\,(\lambda\,P_0 - \mu\,Q_0)$ for some $g \in \mathbb{K}[c]$. Now, if P and Q denote the polynomials defined in Step (3) of the algorithm, we necessarily have:

$$\frac{P}{Q} = \frac{\alpha\,P_0 + \beta\,Q_0}{\delta\,P_0 + \gamma\,Q_0} \in \mathbb{K}(x,y) \setminus \mathbb{K}, \text{ where } \alpha,\beta,\delta,\gamma \in \mathbb{K}.$$

As P_0/Q_0 is a non-composite rational first integral, we deduce that P/Q is also a non-composite rational first integral. Thus, we have $\mathcal{D}(P/Q) = 0$ in Step (4) and the algorithm returns a correct output.
Now suppose that (S) has no rational first integral of degree at most N. In Step (4), the test $\mathcal{D}(P/Q) = 0$ guarantees to return a correct output. In Step (2), we can have an early detection of this situation. Indeed by Proposition 16, if $(\star)$ has no non-trivial solution, then we deduce that (S) has no rational first integral of degree at most N. □

This algorithm fits the first part of our goal as it is entirely based on linear operations: we do not need to solve quadratic equations (see Section 5). However, it is not yet very efficient in practice because computations are done over $\mathbb{K}(c)$. For example, in the first step, a direct calculation shows that, for $n \geq 1$, the coefficient of x^n in the power series solution y_c of (E) satisfying $y_c(0) = c$ is generically a rational function in c of degree $(2n-1)\,d$, whose denominator is generically $A(0,c)^{2\,n-1}$. In what follows, we accelerate things by using only computations over $\mathbb{K}$ instead of computations in $\mathbb{K}(c)$.

4. Efficient algorithms for computing rational first integrals

4.1. **A probabilistic algorithm.** In this section, we present an efficient probabilistic algorithm of Las Vegas type for solving $(\mathcal{P}_N)$. The approach is similar to the one used in the previous section.

Algorithm ProbabilisticRationalFirstIntegral

`Input:` A, $B \in \mathbb{K}[x,y]$ s.t. $A(0,y) \not\equiv 0$, two elements c_1, $c_2 \in \mathbb{K}$ s.t. $A(0,c_i) \neq 0$ for $i = 1, 2$, and a bound $N \in \mathbb{N}$.
`Output:` A non-composite rational first integral of (S) of degree at most N, "None" or "I don't know".

(1) For $i = 1, 2$ do:

(1a) Compute $y_{c_i} \in \mathbb{K}[x]$ of degree at most (N^2+1) s.t. $y_{c_i}(0) = c_i$, and $\frac{dy_{c_i}}{dx} \equiv \frac{B(x,y_{c_i})}{A(x,y_{c_i})} \mod x^{N^2+1}$.

(1b) Compute all non-trivial polynomials $\tilde{M}_i \in \mathbb{K}[x,y]$ of degree $\leq N$ s.t.

$$(\star) : \tilde{M}_i(x, y_{c_i}(x)) \equiv 0 \mod x^{N^2+1}.$$

(1c) If no such $\tilde{M}_i$ exists, then Return "None".
Else let $M_i \in \mathbb{K}[x,y]$ be the primitive part relatively to y of a minimal solution of $(\star)$.

(1d) If $i = 1$, then while $(M_1(0,c_2) = 0$ or $A(0,c_2) = 0)$ do $c_2 = c_2 + 1$.

(2) If $\mathcal{D}(M_1/M_2) = 0$, then Return M_1/M_2. Else Return ["I don't know",$[c_2]$].

Theorem 22. *Algorithm ProbabilisticRationalFirstIntegral terminates and satisfies the following properties:*

- *If it returns M_1/M_2, then it is a non-composite rational first integral of (S) of degree at most N.*
- *If it returns "None", then there is no rational first integral of (S) of degree at most N.*
- *If (S) admits a non-composite rational first integral P/Q of degree at most N and $(Q(0,c_i) : P(0,c_i)) \notin \sigma(P,Q)$ for $i = 1, 2$, then the algorithm returns a non-composite rational first integral of (S) of degree at most N.*

Proof. Let us first prove that the algorithm terminates. This follows directly from the fact that the while loop in Step (1d) terminates after at most $N + d + 1$ steps. Indeed, we just have to avoid the roots of the product $M_1(0,y)\,A(0,y)$ which a univariate polynomial of degree less than $N + d$. It thus remains to check that it is a non-zero polynomial, i.e., $M_1(0,y) \not\equiv 0$. If $M_1(0,y) \equiv 0$, then x divides M_1. As M_1 is the primitive part with respect to y of a minimal solution of $(\star)$, this would imply that $M_1(x,y) = x$ and thus $M_1(x, y_{c_1}(x)) \not\equiv 0 \mod x^{N^2+1}$ which is a contradiction.
Now, if the algorithm returns M_1/M_2, then the test in Step (2) ensures that $\mathcal{D}(M_1/M_2) = 0$ and, by construction, M_1/M_2 is clearly of degree at most N. Furthermore, M_1/M_2 is non-composite. Indeed, if M_1/M_2 is composite, then at least

one of the M_i's is reducible and thus it can not be the primitive part with respect to y of a minimal solution of $(\star)$. Finally Step (1d) certifies that $M_1/M_2 \notin \mathbb{K}$. Indeed, M_2 satisfies $M_2(0, c_2) = 0$, thus if $M_2 = k\,M_1$ with $k \in \mathbb{K}$, then either $k = 0$ or $M_1(0, c_2) = 0$ which is not possible thanks to Step (1d). We have then proved that M_1/M_2 is a non-composite rational first integral of (S) of degree at most N.
If the algorithm returns "None" in Step (1c), then by Proposition 16, (S) has no rational first integral of degree at most N.
Assume finally that (S) admits a non-composite rational first integral P/Q of degree at most N and that $(Q(0, c_i) : P(0, c_i)) \notin \sigma(P, Q)$ for $i = 1, 2$. Then the same strategy as the one used in the proof of Theorem 20 shows that our algorithm returns a non-composite rational first integral of (S).

□

Proposition 23. *Let Ω be a (finite) subset of $\mathbb{K}$ of cardinal $|\Omega|$ greater than $N\,(\mathcal{B}(d)+1)$ and assume that, in Algorithm* ProbabilisticRationalFirstIntegral*, c_1 and c_2 are chosen independently and uniformly at random in Ω. Then, if (S) admits a rational first integral of degree at most N, Algorithm* ProbabilisticRationalFirstIntegral *returns a non-composite rational first integral of (S) of degree at most N with probability at least $\left(1 - \frac{N\,(\mathcal{B}(d)+1)}{|\Omega|}\right)$.*

Proof. It is a straightforward application of Lemma 14, Theorem 22 and Zippel-Schwartz's lemma (see [gGG99, Lemma 6.44]). □

In fact, the "practical" probability will be much better. Indeed, the elements $(\lambda : \mu)$ of the spectrum may be rational or algebraic and hence, the constants c such that $(Q(0, c) : P(0, c)) \in \sigma(P, Q)$ will generally be algebraic. So, if the c_i's are chosen to be rational in the input, then the "bad" values of the c_i's will generally be in very small number. This fact is widely confirmed by experiments.

Now, we study all the different situations that can occur and the corresponding output given by the algorithm ProbabilisticRationalFirstIntegral:

(1) (S) has a non-composite rational first integral P/Q of degree at most N.
   (a) If $(Q(0, c_1) : P(0, c_1)) \notin \sigma(P, Q)$, and $(Q(0, c_2) : P(0, c_2)) \notin \sigma(P, Q)$ then in this situation the algorithm returns a non-composite rational first integral.
   (b) Now, we study the opposite situation: $(Q(0, c_1) : P(0, c_1)) \in \sigma(P, Q)$ or $(Q(0, c_2) : P(0, c_2)) \in \sigma(P, Q)$. If the algorithm computes M_1 and M_2 but M_1/M_2 is not a rational first integral, then it returns "I don't know". A first example where this case is encountered is given in Subsection 6.3. Furthermore, we may be unlucky enough to choose two bad values of the c_i's, i.e., $(Q(0, c_i) : P(0, c_i)) \in \sigma(P, Q)$ for $i = 1, 2$. For example if we consider

$$A(x, y) = -4\,x^3 + 4\,xy^2 + 6\,x^2 - 2\,y^2 - 2\,x,\ B(x, y) = -4\,x^2y + 4\,y^3 + 4\,x\,y - 2\,y,$$

then (S) has a non-composite rational first integral P/Q of degree 2, where $P(x, y) = (y-x)\,(y-x+1)$ and $Q(x, y) = (y+x)\,(y+x-1)$. But if we choose $c_1 = -1$ and $c_2 = 1$, then we will construct two Darboux polynomials $M_1(x, y) = y - x + 1$ and $M_2(x, y) = y + x - 1$ of degree only 1 that are minimal polynomials of y_{c_1} and y_{c_2}. As $\deg(M_1/M_2)$

is strictly smaller than $\deg(P/Q)$, we obtain $\mathcal{D}(M_1/M_2) \neq 0$ and the algorithm returns "I don't know".

(2) (S) does not have a rational first integral with degree at most N.
   (a) If $(\star)$ has no non-trivial solutions, then the algorithm returns "None".
   (b) If $(\star)$ has non-trivial solutions, then the algorithm returns "I don't know". This situation can occur for example when:
      - (S) has no rational first integral but it has Darboux polynomials and the choice of c_1 and c_2 gives two Darboux polynomials. For an example of a derivation without rational first integral but with Darboux polynomials, see [Chè11, Remark 15].
      - (S) has a rational first integral with degree bigger than the given bound N.
        For example, consider the derivation $\mathcal{D} = (x+1)\frac{\partial}{\partial x} - y\frac{\partial}{\partial y}$ and the degree bound $N = 1$. In this situation, the differential equation is $(E) : \frac{dy}{dx} = \frac{-y}{x+1}$ which admits $y_c(x) = \frac{c}{1+x}$ as solution. We set $M(x,y) = \alpha + \beta x + \gamma y$, and then $M(x, y_c(x)) = 0 \mod x^2$ gives $M(x,y) = \gamma(-c + cx + y)$. However, $M(x, y_c(x)) = x^2 \mod x^3$, thus $y_c(x)$ is not a root of M. Here $\mathcal{D}$ admits the rational first integral $y\,(x+1)$ so if we set $N = 2$ in the input, our algorithm returns a non-composite rational first integral of degree 2. In this case we compute $y_c(x) \mod x^5$.

Remark 24. The bivariate polynomials $\tilde{M}_i$'s computed in Step (1b) have total degree at most N so they have $(N+1)(N+2)/2$ coefficients. Note that, if we assume $N \geq 3$, then we have $N^2 + 1 \geq (N+1)(N+2)/2$. It is tempting to try to compute the $\tilde{M}_i$'s using only, say, $(N+1)(N+2)/2 + 2$ terms of the power series. This will make the computation a little bit faster, but then the method becomes only a nice heuristic and may fail.

4.2. **A deterministic algorithm.** Algorithm ProbabilisticRationalFirstIntegral is now turned into a deterministic algorithm. The idea is that if a rational first integral with degree at most N exists then, if we run at most $N\,(\mathcal{B}(d)+1)+1$ times ProbabilisticRationalFirstIntegral, we will get a non-composite rational first integral of degree at most N.

Algorithm DeterministicRationalFirstIntegral

`Input:` A, $B \in \mathbb{K}[x,y]$ s.t. $A(0,y) \not\equiv 0$ and a bound $N \in \mathbb{N}$.
`Output:` A non-composite rational first integral of (S) of degree $\leq N$ or "None".

(1) Let $\Omega := \emptyset$.

(2) While $|\Omega| \leq 2\,N\,(\mathcal{B}(d)+1)+2$ do
   (a) Choose two random elements c_1, $c_2 \in \mathbb{K}\backslash\Omega$ s.t. $c_1 \neq c_2$ and $A(0,c_i) \neq 0$ for $i = 1, 2$.
   (b) $F :=$ ProbabilisticRationalFirstIntegral$(A, B, (c_1, c_2), N)$.
   (c) If $F =$"None", then Return "None".

(d) Else if F =["I don't know",$[e_2]$], then $\Omega := \Omega \cup \{c_1, e_2\}$ and go to Step (2).
(e) Else Return F.

(3) Return "None".

Theorem 25. *Algorithm DeterministicRationalFirstIntegral is correct: it returns a rational first integral of degree at most N if and only if it exists, and it returns "None" if and only if there is no rational first integral of degree at most N.*

Proof. Assume that (S) has a non-composite rational first integral P/Q with degree at most N. If F ="I don't know" in Step (2), then from Theorem 22, at least one of the c_i's satisfies $(Q(0, c_i) : P(0, c_i)) \in \sigma(P, Q)$. The number of such "bad" values of the c_i's is bounded by $N(\mathcal{B}(d) + 1)$ by Lemma 14. Hence if we repeat ProbabilisticRationalFirstIntegral at least $N(\mathcal{B}(d) + 1) + 1$ times, then we will get a good pair (c_1, c_2) and by Theorem 22, the probabilistic algorithm will then return a non-composite rational first integral of degree at most N.
Now assume that (S) has no rational first integral of degree at most N. Then by Theorem 22, ProbabilisticRationalFirstIntegral returns "None" or "I don't know".
If in Step (2), F="None", then we have a correct output. Now if F="I don't know", then the algorithm uses again ProbabilisticRationalFirstIntegral with new values of the c_i's and, after at most $N(\mathcal{B}(d) + 1) + 1$ trials, it returns "None" which is the correct output. □

5. Complexity analysis and algorithmic issues

In this section, we describe how the different steps of algorithms ProbabilisticRationalFirstIntegral and DeterministicRationalFirstIntegral can be performed efficiently and we study their arithmetic complexities. For the complexity issues, we focus on the dependency on the degree bound N and we recall that we assume that $N \geq d$, where $d = \max(\deg(A), \deg(B))$ denotes the degree of the polynomial vector field. More precisely, we suppose that d is fixed and N tends to infinity.

All the complexity estimates are given in terms of arithmetic operations in $\mathbb{K}$. We use the notation $f \in \tilde{\mathcal{O}}(g)$: roughly speaking, it means that f is in $\mathcal{O}(g \log^m(g))$ for some $m \geq 1$. For a precise definition, see [gGG99, Definition 25.8]. We suppose that the Fast Fourier Transform can be used so that two univariate polynomials with coefficients in $\mathbb{K}$ and degree bounded by D can be multiplied in $\tilde{\mathcal{O}}(D)$, see [gGG99]. We further assume that two matrices of size n with entries in $\mathbb{K}$ can be multiplied using $\mathcal{O}(n^\omega)$, where $2 \leq \omega \leq 3$ is the matrix multiplication exponent, see [gGG99, Ch. 12]. We also recall that a basis of solutions of a linear system composed of m equations and $n \leq m$ unknowns over $\mathbb{K}$ can be computed using $\mathcal{O}(m\, n^{\omega-1})$ operations in $\mathbb{K}$, see [BP94, Chapter 2].

5.1. **Computation of a regular point.** In the algorithms given in the previous sections, we have to choose a regular point for the differential equation (E), i.e., a point x_0 satisfying $A(x_0, y) \not\equiv 0$. To achieve this, we can start from the point $x_0 = 0$, evaluate $A(x, y)$ at $x = x_0$. If $A(x_0, y) \not\equiv 0$, then we are done. Else, we shift x_0 by one to get $x_0 = 1$ and we iterate the process. Note that the number of iterations is at most d. Consequently, this step can be performed by evaluating d polynomials (namely the coefficients of $A(x, y)$ viewed as polynomials in the

variable y) of degree bounded by d at d points ($x_0 = 0, 1, 2, \ldots, d-1$). This can thus be done in $\tilde{\mathcal{O}}(d^2)$ arithmetic operations, see [gGG99, Corollary 10.8]. This is why, in our algorithms, we always suppose, at neglectable cost and without loss of generality, that $A(0, y) \not\equiv 0$.

5.2. **Power series solutions of (E).** In Step (1) of the algorithm ProbabilisticRationalFirstIntegral, we compute the N^2+1 first terms of the power series solution of (E) satisfying a given initial condition. Using the result of Brent and Kung (see [BK78, Theorem 5.1]) based on formal Newton iteration, this can be done using $\tilde{\mathcal{O}}(d\,N^2)$ arithmetic operations, see also [BCO+07].

5.3. **Guessing the minimal polynomial of an algebraic power series.** We shall now give a method for solving Problem ($\star$) in Step (1b) of Algorithm ProbabilisticRationalFirstIntegral. The problem is the following: given the first N^2+1 terms of a power series $\hat{y}(x)$, find (if it exists), a bivariate polynomial $M \in \mathbb{K}[x, y]$, with minimal degree in y, such that $M(x, \hat{y}(x)) \equiv 0 \mod x^{N^2+1}$. This can be handled by an undetermined coefficients approach as follows:

Algorithm GuessMinimalPolynomial

`Input:` A *polynomial* $\hat{y} \in \mathbb{K}[x]$ s.t. $\deg(\hat{y}) \leq (N^2+1)$, with $N \in \mathbb{N}$.
`Output:` A minimal solution of ($\star$) with degree $\leq N$ or "None".

(1) Let $M(x, y) = \sum_{i=0}^{N} \left(\sum_{j=0}^{N-i} m_{i,j}\, x^j \right) y^i$ be an ansatz for the bivariate polynomial that we are searching for.

(2) Construct the linear system ($\mathcal{L}$) for the $m_{i,j}$'s given by:

$$M(x, \hat{y}(x)) = \sum_{i=0}^{N} \left(\sum_{j=0}^{N-i} m_{i,j}\, x^j \right) \hat{y}(x)^i \equiv 0 \mod x^{N^2+1}.$$

(3) If ($\mathcal{L}$) does not have a non-trivial solution, then Return "None".

(4) Else compute a row-echelon form of a basis of solutions of ($\mathcal{L}$) to find a solution $M(x, y)$ of minimal degree in y and Return it.

Proposition 26. *Algorithm GuessMinimalPolynomial is correct. If we suppose that $N \geq 3$, then it uses at most $\tilde{\mathcal{O}}(N^{2\omega})$ arithmetic operations in $\mathbb{K}$.*

Proof. The correctness of the algorithm is straightforward. Let us study its arithmetic complexity. To construct the linear system ($\mathcal{L}$), we have to compute $\hat{y}(x)^i \mod x^{N^2+1}$ for $i = 0, \ldots, N$. This can be done in $\tilde{\mathcal{O}}(N^3)$ arithmetic operations. The linear system ($\mathcal{L}$) has N^2+1 equations and $(N+1)(N+2)/2 = \mathcal{O}(N^2)$ unknowns $m_{i,j}$'s. Note that we assume $N \geq 3$ so that $N^2+1 \geq (N+1)(N+2)/2$. It can thus be solved using $\mathcal{O}(N^2 (N^2)^{\omega-1})$ operations. Finally, in Step (4), the row-echelon form can be computed using at most $\tilde{\mathcal{O}}(N^{2\,\omega})$ arithmetic operations (see [BP94, Chapter 3]) since the dimension of a basis of solutions of ($\mathcal{L}$) does not exceed $\mathcal{O}(N^2)$, which ends the proof. □

5.4. **Total cost of our algorithms.**

Theorem 27. *Algorithm* ProbabilisticRationalFirstIntegral *uses at most* $\tilde{\mathcal{O}}(N^{2\omega})$ *arithmetic operations in* $\mathbb{K}$*, when* N *tends to infinity and* d *is fixed.*

Proof. In Subsection 5.2, we have seen that Step (1a) can be performed in at most $\tilde{\mathcal{O}}(d\,N^2)$ arithmetic operations. Then, using Algorithm GuessMinimalPolynomial, Step (1b) can be performed in $\tilde{\mathcal{O}}(N^{2\,\omega})$ operations in $\mathbb{K}$, see Subsection 5.3. In Step (1c), we have to compute the primitive part relatively to y of a minimal solution of $(\star)$. This reduces to computing N gcd's of univariate polynomials of degree at most N which can be done in $\mathcal{O}(N^3)$ operations in $\mathbb{K}$ (and even faster using half-gcd techniques). In Step (1d), we must avoid the roots of $M_1(0,y)\,A(0,y)$ thus we need to run the while loop at most $d+N+1$ times. In this loop we evaluate univariate polynomials with degree at most d and N, thus it uses at most $\tilde{\mathcal{O}}((d+N)^2)$ arithmetic operations. Finally, we test if $\mathcal{D}(M_1/M_2)=0$ which costs $\tilde{\mathcal{O}}((d+N)^2)$ arithmetic operations since $N \geq d$. Indeed, we multiply bivariate polynomials of degree at most N and we add bivariate polynomials of degree at most $d+2N-1$. □

Corollary 28. *The deterministic algorithm* DeterministicRationalFirstIntegral *can be done using at most* $\tilde{\mathcal{O}}(d^2\,N^{2\omega+1})$ *arithmetic operations, when* N *tends to infinity and* d *is fixed.*

In the previous statement, even if d is fixed, we mention it in the complexity in order to emphasize on the number of iterations of the probabilistic algorithm.

Proof. This estimate is straightforward from Theorem 27 since Algorithm DeterministicRationalFirstIntegral calls at most $N\,(\mathcal{B}(d)+1)+1$ times the algorithm ProbabilisticRationalFirstIntegral. □

5.5. **Faster heuristic using Padé-Hermite approximation.** The algorithm GuessMinimalPolynomial developed in Subsection 5.3 uses an undetermined coefficients method to compute a minimal solution of $(\star)$ in Step (1b) of Algorithm ProbabilisticRationalFirstIntegral. It consists in finding (if it exists) the minimal polynomial of a power series. In the present section, we propose another approach to solve that problem using Padé-Hermite approximation, see [BL94].
Indeed, the problem of computing a bivariate polynomial annihilating a power series can be handled by means of computing a Padé-Hermite approximant, see [Sha74, Sha78]. More precisely, given a power series $\hat{y}(x)$, if there exists a bivariate polynomial M of degree N such that $M(x,\hat{y}(x))=0$, then the coefficients of the powers of y are a Padé-Hermite approximant of type $(N,N-1,\ldots,0)$ of the vector of power series $(1,\hat{y}(x),\ldots,\hat{y}(x)^N)^T$. Computing such a Padé-Hermite approximant provides a polynomial $\tilde{M}$ satisfying $\tilde{M}(x,\hat{y}(x)) \equiv 0 \mod x^\sigma$ where $\sigma = N\,(N+1)/2+N-1$. Unfortunately $\sigma < N^2+1$ so that we have no way to ensure, using Lemma 18, that the Padé-Hermite approximant computed satisfies $\tilde{M}(x,\hat{y}(x))=0$. Consequently, using this method to compute the M_i's in Step (1b) of Algorithm ProbabilisticRationalFirstIntegral only provides a heuristic.

Proposition 29. *Using Padé-Hermite approximation in Step (1b), Algorithm* ProbabilisticRationalFirstIntegral *becomes a heuristic for computing a non-composite rational first integral of* (S) *of degree at most* N *using only* $\tilde{\mathcal{O}}(N^{\omega+2})$ *arithmetic operations.*

Proof. Beckermann-Labahn's algorithm (see [BL94]) computes a Padé-Hermite approximant of type $(N, N-1, \ldots, 1)$ of the vector of power series $(1, \hat{y}(x), \ldots, \hat{y}(x)^N)^T$ in $\tilde{\mathcal{O}}(N^\omega\,\sigma)$ arithmetic operations, where $\sigma = N\,(N+1)/2+N-1$. Using the proof of Theorem 27, we obtain the desired complexity estimate. □

6. Implementation and experiments

The algorithms developed in the previous sections have been implemented in a Maple package called RationalFirstIntegrals. It is available with some examples at http://www.ensil.unilim.fr/~cluzeau/RationalFirstIntegrals.html.

Our implementation of the heuristic proposed in Subsection 5.5 is called HeuristicRationalFirstIntegral. It uses the gfun package [SZ94][2] and more precisely its seriestoalgeq command to search for a bivariate polynomial annihilating the power series computed using Padé-Hermite approximation.

We shall now illustrate our implementation and give some timings[3].

6.1. Comparison to previous methods.

We start by comparing our implementation DeterministicRationalFirstIntegral to two previous methods, namely:

(1) the *naive* approach which consists in using the method of undetermined coefficients to search for two polynomials P and Q of degree at most N satisfying $\mathcal{D}(P)\,Q - P\,\mathcal{D}(Q) = 0$. This implies solving a system of quadratic equations in the coefficients of P and Q. In our implementation, we use the solve command of Maple to solve the quadratic system,
(2) the approach developed in [Chè11] based on the *ecstatic curve*.

Consider the planar polynomial vector field given by $A(x,y) = -7\,x + 22\,y - 55$ and $B(x,y) = -94\,x + 87\,y - 56$ which has no rational first integral of degree less than 6. The following table compares the timings (in seconds) of the different implementations for proving the non-existence of a rational first integral of degree less than $N = 2, \ldots, 6$.

N \ Method	DeterministicRFI	Ecstatic curve	Naive method
2	0.043	0.003	0.257
3	0.006	0.024	0.043
4	0.016	3.310	4.438
5	0.041	74.886	16.202
6	0.140	1477.573	88.482

If we now consider the vector field given by the polynomials $A(x,y) = x + 2$ and $B(x,y) = -x^2 - 2\,x\,y - y^2 - 2\,x - y - 2$ which admits the rational first integral $\frac{x^2+x\,y-2}{x+y+1}$ of degree 2, we obtain the following timings (in seconds) depending on the degree bound N given in the input:

[2] http://perso.ens-lyon.fr/bruno.salvy/?page_id=48
[3] All the computations were made on a 2.7 GHz Intel Core i7

N \ Method	DeterministicRFI	Ecstatic curve	Naive method
2	0.012	0.003	0.137
3	0.019	0.019	1.961
4	0.042	0.283	5.398
5	0.087	1.662	22.580
6	1.276	8.491	80.491

In the latter table, the timings indicated for the "ecstatic curve method" correspond only to the computation of the Nth ecstatic curve (which will be zero in all cases as there exists a rational first integral of degree 2) and not to the entire computation of a rational first integral of degree at most N which requires some more computations, see [Chè11, Subsection 5.2] for more details. The output of the two other methods consists in a rational first integral of degree 2.

The timings presented in this subsection illustrate that our implementation of DeterministicRationalFirstIntegral is significantly faster than our implementations of the two previous methods considered both in the case where there exists no rational first integral and in the case where there exists a rational first integral. This is coherent with the complexity analysis developed in this article.

6.2. **Generic polynomial vector fields.** If we choose at random two bivariate polynomials A and B, then the associated planar polynomial vector field has generically no rational first integral. In this subsection, we show that our implementation of DeterministicRationalFirstIntegral detects quickly the non-existence of rational first integral of these generic polynomial vector fields. The following table of timings is constructed as follows: for $d = 1, \ldots, 10$, we generate two randomized bivariate polynomials A and B of degree d using the randpoly command of Maple and we check that $A(0, y) \not\equiv 0$. Then, we run DeterministicRationalFirstIntegral with $N = d, \ldots, 10$ and we indicate the timings (in seconds) for detecting the non-existence of a rational first integral of degree at most N, i.e., for returning the output "None".

d \ N	1	2	3	4	5	6	7	8	9	10
1	0.007	0.043	0.006	0.017	0.049	0.157	0.294	1.054	2.275	5.010
2	-	0.044	0.008	0.022	0.070	0.214	0.588	1.055	4.644	11.249
3	-	-	0.008	0.161	0.084	0.273	0.498	1.458	5.267	7.676
4	-	-	-	0.043	0.107	0.577	0.298	2.354	9.688	9.10
5	-	-	-	-	0.133	0.466	0.812	2.439	3.054	8.012
6	-	-	-	-	-	0.533	0.967	1.557	5.946	5.031
7	-	-	-	-	-	-	0.663	1.323	4.724	9.834
8	-	-	-	-	-	-	-	2.468	3.551	5.756
9	-	-	-	-	-	-	-	-	7.898	18.127
10	-	-	-	-	-	-	-	-	-	18.295

6.3. **Our probabilistic algorithm may fail.** We now illustrate one particular case where our probabilistic algorithm ProbabilisticRationalFirstIntegral fails and returns "I don't know". Consider the polynomial vector field given by the polynomials

$$A(x,y) = x^6 - x^5 + 2\,x^4y - x^4 + 2\,x^3y - x^2y^2 + xy^2 - x^2 - 2\,xy + y^2 + x - 2\,y + 1,$$

$$B(x,y) = -x^6+2\,x^5y-3\,x^4y+4\,x^3y^2+3\,x^4-4\,x^3y+3\,x^2y^2-2\,xy^3+y^3-3\,x^2+2\,xy-y^2-y+1,$$

which admits the rational first integral of degree 4

$$F(x,y) = \frac{P(x,y)}{Q(x,y)} = \frac{(y-x)\left(x^2+y-1\right)}{x^4+y^2-1}.$$

If we run ProbabilisticRationalFirstIntegral with the bound $N = 4$ and $c_1 = 0$ or $c_2 = 0$ in the input, then we get "I don't know". The reason why our algorithm fails is that $(Q(0,0) : P(0,0)) = (-1 : 0) \in \sigma(P,Q)$ since $-P(x,y) = -\,(y-x)\left(x^2+y-1\right)$ is a reducible polynomial (and also a polynomial of degree less than $N = 4$). Of course, running ProbabilisticRationalFirstIntegral with values of c_1 and c_2 such that $(Q(0,c_i) : P(0,c_i)) \notin \sigma(P,Q)$ for $i = 1, 2$ provides the correct output, i.e., a rational first integral of degree $N = 4$; see the explanations at the end of Subsection 4.1. The deterministic algorithm DeterministicRationalFirstIntegral calls recursively ProbabilisticRationalFirstIntegral and exploits the fact that there only exists a finite number of such bad values of the c_i's. So in this example, it returns correctly a rational first integral of degree $N = 4$.

6.4. **Examples from the work of Ferragut and Giacomini.** Let us consider [FG10, Example 1], where we have

$$A(x,y) = 6\,x^4 + 27\,x^3 - 9\,x^2y + 42\,x^2 - 24\,xy + 4\,y^2 + 21\,x - 7\,y + 4,$$

and

$$B(x,y) = 18\,x^4 + 99\,x^3 - 39\,x^2y + 2\,xy^2 + 150\,x^2 - 80\,xy + 12\,y^2 + 71\,x - 21\,y + 12.$$

A first integral of degree 4 was found in 12 seconds using their algorithm (see [FG10]) which was a notable improvement on previous methods. In comparison, running HeuristicRationalFirstIntegral (or DeterministicRationalFirstIntegral) with $N = 4$ we get such a rational first integral $F = P/Q$ in 0.022 seconds, where

$$\begin{aligned} P(x,y) = {} & -216\,x^4 + 144\,x^3\,y - 24\,x^2\,y^2 - 720\,x^3 + 528\,x^2\,y - 144\,x\,y^2 \\ & +16\,y^3 + 8868\,x^2 + 432\,x\,y - 72\,y^2 + 28548\,x - 9516\,y + 9580, \end{aligned}$$

and

$$\begin{aligned} Q(x,y) = {} & 513\,x^4 - 342\,x^3\,y + 57\,x^2\,y^2 + 1710\,x^3 - 1254\,x^2\,y + 342\,x\,y^2 \\ & -38\,y^3 - 10869\,x^2 - 1026\,x\,y + 171\,y^2 - 37224\,x + 12408\,y - 12560. \end{aligned}$$

Two observations allow us to obtain a more compact form for F. First, looking at the syzygy in the leading term in x^4, we see that

$$513\;P(x,y) + 216\;Q(x,y) = 2201580\;(x^2 + 3\,x - y + 1).$$

Secondly, the discriminant of $P - c\;Q$ shows that $117\;P + 89\;Q$ has a multiple factor, namely

$$117\;P(x,y) + 89\;Q(x,y) = 755\;\left(3\,x^2 + 6\,x - 2\,y + 1\right)(2 + 3\,x - y)^2\,.$$

It follows that we have the following "nicer" rational first integral:

$$\tilde{F}(x,y) = \frac{x^2+3\,x-y+1}{(3\,x^2+6\,x-2\,y+1)\,(2+3\,x-y)^2}.$$

This simplification heuristics (using the spectrum) of the expression of a rational first integral to a more compact form can be obtained automatically by running the command SimplifyRFI of our package RationalFirstIntegrals.

In this example, the generic algorithm GenericRationalFirstIntegral run with $N=4$ takes 0.342 seconds to compute a rational first integral; we see that, though it is 15 times slower than HeuristicRationalFirstIntegral (or DeterministicRationalFirstIntegral), it still has good performances on relatively small degrees.

Let us now have a look at the polynomial vector field given by

$$A(x,y) = -18\,x^8y^8 - 20\,x^6y^9 - 6\,x^2y^{12} + 24\,x^{10}y^3 - 6\,x^4y^9 - 4\,y^{13} - 3\,x^{12} - 7\,x^2y^{10},$$

$$B(x,y) = 2\,x\left(-16\,x^6y^9 + 8\,x^{14} - 18\,x^4y^{10} - 2\,y^{13} + 10\,x^8y^4 - 2\,x^2y^{10} - 2\,x^{10}y - 3\,y^{11}\right),$$

considered by A. Ferragut in one of his talks concerning [FG10]. It admits a rational first integral of degree 18. We have run our implementations of HeuristicRationalFirstIntegral and ProbabilisticRationalFirstIntegral with the given bounds $N=3$, 6, 9, 12, 15, and 18 in the input. The following table presents the outputs and the timings (in seconds) that we have obtained:

Algorithm \ N	3	6	9	12	15	18
Output Heuristic	?	?	?	?	?	F
Time Heuristic	0.031	1.672	29.858	319.799	1735.189	19.548
Output Probabilistic	?	None	None	None	None	F
Time Probabilistic	0.015	0.066	1.023	5.386	28.714	252.842

In the latter table, ? means that our implementation returns "I don't know" and $F=P/Q$ is the rational first integral of degree 18 given by

$$P(x,y) = -24\,x^2y^9 + 24\,x^{10} - 24\,y^{10},$$

$$Q(x,y) = 8\,x^{18} - 24\,x^{12}y^4 + 12\,x^{14}y + 24\,x^6y^8 - 24\,x^8y^5 + 6\,x^{10}y^2 - 8\,y^{12} + 44\,x^2y^9 - 32\,x^{10} - 6\,x^4y^6 + 32\,y^{10} + x^6y^3.$$

Note that we obtain approximatively the same timings if we run the deterministic algorithm DeterministicRationalFirstIntegral instead of ProbabilisticRationalFirstIntegral. We can remark that our implementation of HeuristicRationalFirstIntegral is faster in this example than our implementation of ProbabilisticRationalFirstIntegral when there exists a rational first integral whereas ProbabilisticRationalFirstIntegral is much faster at discarding cases when no rational first integral exists. Moreover, we can see that, in this example, HeuristicRationalFirstIntegral only returns "I don't know" for $N=6$, 9, 12, 15 whereas in these cases, ProbabilisticRationalFirstIntegral proves that there is no rational first integral of degree at most N. Note that these two drawbacks of HeuristicRationalFirstIntegral come from our implementation, which uses the command seriestoalgeq of the GFUN package, and not from the algorithm itself.

In this example, if we replace Q by $P + \frac{3}{4}\,Q$, we obtain a new rational first integral $\tilde{F} = \frac{P}{P+\frac{3}{4}\,Q}$ which has a "nicer" (more compact) form

$$\tilde{F}(x,y) = \frac{x^2y^9 - x^{10} + y^{10}}{\left(2\,x^6 - 2\,y^4 + x^2y\right)^3}.$$

This simplification of the expression of the rational first integral P/Q to a more compact form is obtained with the command SimplifyRFI of our package.

6.5. **A hypergeometric example.** Consider the family of polynomial vector fields given by $A = 4\,n^2\,(x-1)\,(x+1)$ and $B = 1 + \left(-4\,n^2\,x^2 + 4\,n^2\right)y^2 - 4\,x\,y\,n^2$. For each integer $n \in \mathbb{N}^*$, it admits a rational first integral of degree $N = 4\,n + 1$. This system is derived from the Riccati equation of a standard hypergeometric equation with a finite dihedral differential Galois group, see [vHW05]. The following table contains the timings (in seconds) for HeuristicRationalFirstIntegral to find a rational first integral of degree $N = 4\,n + 1$ when it is run with $N = 4\,n + 1$.

n	2	4	6	8	10
Degree N	9	17	25	33	41
Time Heuristic	0.540	12.548	118.804	592.494	3247.325

In short, it takes 2 minutes to compute a rational first integral of degree 25 and 52 minutes to compute a rational first integral of degree 41 for this family of examples.

6.6. **An Abel equation.** We consider the rationally integrable Abel differential equation (3) in the article of Gine and Llibre [GL10]. It corresponds to the polynomial vector field given by $A(x,y) = x\,(8\,y - 9)$ and $B(x,y) = 3\,y^2 - x - 3\,y$. A rational first integral of degree 12 is computed in 4.142 seconds by HeuristicRationalFirstIntegral and in 31.976 seconds by DeterministicRationalFirstIntegral if they are both run with $N = 12$. The rational first integral returned by HeuristicRationalFirstIntegral is given by P/Q with

$$\begin{aligned} P(x,y) = {} & 80\,y^{12} + 480\,xy^{10} + 1200\,x^2y^8 - 1440\,xy^9 + 1600\,x^3y^6 - 5760\,x^2y^7 + 1200\,x^4y^4 \\ & - 8640\,x^3y^5 + 8640\,x^2y^6 + 480\,x^5y^2 - 5760\,x^4y^3 + 13248\,x^3y^4 + 80\,x^6 - 1440\,x^5y \\ & + 576\,x^4y^2 - 13248\,x^3y^3 - 4032\,x^5 + 36288\,x^4y - 27216\,x^4 \end{aligned}$$

and

$$\begin{aligned} Q(x,y) = {} & 3\,y^{12} + 18\,xy^{10} + 45\,x^2y^8 - 54\,xy^9 + 60\,x^3y^6 - 216\,x^2y^7 + 45\,x^4y^4 - 324\,x^3y^5 \\ & + 324\,x^2y^6 + 18\,x^5y^2 - 216\,x^4y^3 + 680\,x^3y^4 + 3\,x^6 - 54\,x^5y + 388\,x^4y^2 - 680\,x^3y^3 \\ & + 32\,x^5 - 288\,x^4y + 216\,x^4 \end{aligned}$$

Using the SimplifyRFI procedure, we find a rational first integral written in a more compact form:

$$F(x,y) = \frac{\left(y^4 + 2\,y^2x + x^2 - 6\,yx\right)^3}{x^3\left(4\,y^4 + 8\,y^2x - 4\,y^3 + 4\,x^2 - 36\,yx + 27\,x\right)}$$

7. Computation of Darboux polynomials

In this section, we show how the approach used above for computing rational first integrals of (S) of degree bounded by a fixed $N \in \mathbb{N}$ can be slightly modified for computing all irreducible Darboux polynomials for the derivation $\mathcal{D}$ associated with (S) of degree at most N.

In the output of our algorithms, irreducible Darboux polynomials in $\overline{\mathbb{K}}[x,y]$ will be given by $M(c,x,y) \in \mathbb{K}[c,x,y]$ and $f(c) \in \mathbb{K}[c]$. The univariate polynomial $f(c)$ is irreducible in $\mathbb{K}[c]$ and for all roots c_i of $f(c)$, we have an irreducible Darboux polynomial $M(c_i,x,y) \in \overline{\mathbb{K}}[x,y]$.

7.1. **A deterministic algorithm.** In this section we give a deterministic algorithm for computing all irreducible Darboux polynomials for the derivation $\mathcal{D}$ associated with (S) of degree at most N. This algorithm is divided into two steps. First, we compute all irreducible Darboux polynomials $M(x,y)$ such that $M(0,y) \notin \mathbb{K}$: this is the task of Algorithm IrreducibleDarbouxPolynomialsPartial below applied to A and B. Then, in a second step, we show how we can compute the missing Darboux polynomials (those satisfying $M(0,y) \in \mathbb{K}$) by applying IrreducibleDarbouxPolynomialsPartial to relevant polynomials constructed from A and B by a change of coordinates.

In these algorithms we suppose $A(0,y) \not\equiv 0$ and $A(0,y)$, $B(0,y)$ coprime. We can easily reduce our study to this situation. We have already explained how we can get $A(0,y) \not\equiv 0$. Now, we just have to remark that the second condition corresponds to the choice of an element which is not a root of the resultant $\mathrm{Res}_y(A(x,y),B(x,y))$. Thus after a finite number of shifts, we can assume that $A(0,y) \not\equiv 0$ and that $A(0,y)$ and $B(0,y)$ are coprime. In particular, this implies that x is not a Darboux polynomial and if M is a Darboux polynomial, then $M(0,y) \not\equiv 0$ in $\mathbb{K}[y]$. We also assume that $\mathcal{D}$ would have no rational first integral with degree at most N. Indeed, from Theorem 6, in this situation $\mathcal{D}$ has an infinite number of irreducible Darboux polynomials. We can check this hypothesis with the previous algorithms.

Algorithm IrreducibleDarbouxPolynomialsPartial

`Input:` A, $B \in \mathbb{K}[x,y]$ s.t. $A(0,y) \not\equiv 0$, $A(0,y)$, $B(0,y)$ coprime, and a bound $N \in \mathbb{N}$ such that (S) has no rational first integral of degree at most N.
`Output:` The set of all irreducible Darboux polynomials M for the derivation $\mathcal{D}$ such that $\deg(M) \leq N$ and $M(0,y) \notin \mathbb{K}$.

(1) $\mathcal{E} := \emptyset$.

(2) For an indeterminate c, compute the polynomial $y_c \in \mathbb{K}(c)[x]$ of degree at most (N^2+1) s.t. $y_c(0) = c$ and $\frac{dy_c}{dx} \equiv \frac{B(x,y_c)}{A(x,y_c)} \mod x^{N^2+1}$.

(3) For an indeterminate c, compute the polynomial $x_c \in \mathbb{K}(c)[y]$ of degree at most (N^2+1) s.t. $x_c(c) = 0$ and $\frac{dx_c}{dy} \equiv \frac{A(x_c,y)}{B(x_c,y)} \mod y^{N^2+1}$.

(4) Let $M(x,y) = \sum_{i=0}^{N} \left(\sum_{j=0}^{N-i} m_{i,j}\, x^j \right) y^i$ be an ansatz for the Darboux polynomials that we are searching for.

(5) Construct the linear system $\mathcal{L}_1(c)$ for the $m_{i,j}$'s given by:

$$M(x, y_c(c,x)) \equiv 0 \mod x^{N^2+1}.$$

(6) Construct the linear system $\mathcal{L}_2(c)$ for the $m_{i,j}$'s given by:

$$M(x_c(c,y),y) \equiv 0 \mod y^{N^2+1}.$$

(7) For $k = 1$, 2 do:

  (a) Clear the denominator in $\mathcal{L}_k(c)$.
  (b) Compute the Smith normal form of $\mathcal{L}_k(c)$. Let $\mathcal{P}_k(c)$ be the last invariant factor of $\mathcal{L}_k(c)$.
  (c) Factorize $\mathcal{P}_k(c)$ over $\mathbb{K}$: $\mathcal{P}_k(c) = \prod_{i=1}^{s_k} \mathcal{P}_{k,i}(c)$.
  (d) For i from 1 to s_k do:
    (i) Set $\mathbb{K}[c_i] := \mathbb{K}[c]/(\mathcal{P}_{k,i}(c))$.
    (ii) Compute a solution of $\mathcal{L}(c_i)$ s.t. the corresponding polynomial $M_{k,i}$ has minimal degree in y and is primitive w.r.t. y.
    (iii) If $\gcd(\mathcal{D}(M_{k,i}), M_{k,i}) = M_{k,i}$, then $\mathcal{E} := \mathcal{E} \cup \{[M_{k,i}(c,x,y), \mathcal{P}_{k,i}(c)]\}$.

(8) Return $\mathcal{E}$.

Proposition 30. *Algorithm* IrreducibleDarbouxPolynomialsPartial *is correct.*

Proof. Let M be an irreducible Darboux polynomial such that $M(0,y) \notin \mathbb{K}$ and c_M be a root of $M(0,y)$. Then we have: $A(0,c_M) \neq 0$ or $B(0,c_M) \neq 0$ because $A(0,y)$ and $B(0,y)$ are assumed to be coprime.
If $A(0,c_M) \neq 0$ and $M(0,c_M) = 0$, then M admits a root $y_{c_M} \in \overline{\mathbb{K}(x)}$ such that $y_{c_M}(0) = c_M$. Then, from Proposition 17, y_{c_M} is a power series solution of (E). Thus c_M is a root of $\mathcal{P}_1(c)$. Then, by Lemma 18, M is constructed in Step (7(d)ii). If for a constant c_M, we have $B(0,c_M) \neq 0$ and $M(0,c_M) = 0$, then the previous arguments used with $\mathcal{P}_2(c)$ show that M is also constructed. □

In the algorithm IrreducibleDarbouxPolynomialsPartial, we compute irreducible Darboux polynomials M such that $M(0,y) \notin \mathbb{K}$. Indeed, the algorithm finds a irreducible Darboux polynomial M if and only if the curve $M(x,y) = 0$ and the line $x = 0$ have an intersection point. Now, we show how to get irreducible Darboux polynomials such that $M(0,y) \in \mathbb{K}$. The idea is to use a change of coordinates in order to get a new polynomial $\tilde{M}$ such that $\tilde{M}(0,y)$ has a root. If $M(0,y) \in \mathbb{K}$, then M has a root at infinity. Thus we consider the following change of coordinates: we set

$$A^\sharp(x,y,z) = A\Big(\frac{x}{z},\frac{y}{z}\Big)\, z^d,\ B^\sharp(x,y,z) = B\Big(\frac{x}{z},\frac{y}{z}\Big)\, z^d,\ M^\sharp(x,y,z) = M\Big(\frac{x}{z},\frac{y}{z}\Big)\, z^k,$$

where $k = \deg(M)$, and we consider the following polynomials:

$$\tilde{A}(y,z) = A^\sharp(1,y,z),\ \tilde{B}(y,z) = B^\sharp(1,y,z),\ \tilde{M}(y,z) = M^\sharp(1,y,z).$$

A straightforward computation shows that:

Lemma 31. *With the above notation, if M is a Darboux polynomial for the derivation $\mathcal{D} = A(x,y)\frac{\partial}{\partial x} + B(x,y)\frac{\partial}{\partial y}$, then $\tilde{M}$ is a Darboux polynomial for the derivation*

$$\tilde{\mathcal{D}} = \Big(-y\,\tilde{A}(y,z) + \tilde{B}(y,z)\Big)\,\frac{\partial}{\partial y} - \tilde{A}(y,z)\,z\,\frac{\partial}{\partial z}.$$

Furthermore, if $M(0,y) \in \mathbb{K} \setminus \{0\}$, then $\tilde{M}(0,z) \notin \mathbb{K}$.

We deduce the following algorithm:

Algorithm IrreducibleDarbouxPolynomials

`Input:` A, $B \in \mathbb{K}[x,y]$ s.t. $A(0,y) \not\equiv 0$, $A(0,y)$, $B(0,y)$ coprime, $\tilde{B}(0,z) \not\equiv 0$, $\tilde{A}(0,y)$ and $\tilde{B}(0,y)$ coprime, and a bound $N \in \mathbb{N}$ such that (S) has no rational first integral of degree at most N.
`Output:` The set of all irreducible Darboux polynomials M for the derivation $\mathcal{D}$ such that $\deg(M) \leq N$.

(1) $\mathcal{E} :=$ IrreducibleDarbouxPolynomialsPartial(A, B, N).
(2) $\mathcal{E}' :=$ IrreducibleDarbouxPolynomialsPartial$(-y\,\tilde{A} + \tilde{B}, -\tilde{A}\,z, N)$.
(3) For all $[\tilde{M}(c,y,z), \mathcal{P}(c)] \in \mathcal{E}'$ do:
    (a) $M(c,x,y) := \tilde{M}(c, \frac{y}{x}, \frac{1}{x})\, x^{\deg(M)}$.
    (b) Add $[M(c,x,y), \mathcal{P}(c)]$ to $\mathcal{E}$.
(4) Return $\mathcal{E}$.

For the same reasons as before, using a finite number of shifts we can suppose that the hypotheses "$A(0,y) \not\equiv 0$, $A(0,y)$, $B(0,y)$ coprime, $\tilde{B}(0,z) \not\equiv 0$, $\tilde{A}(0,y)$, $\tilde{B}(0,y)$ coprime" are satisfied so that these conditions are not restrictive.

As a direct consequence of Proposition 30 and Lemma 31, we obtain the following result.

Proposition 32. *Algorithm IrreducibleDarbouxPolynomials is correct.*

7.2. **A probabilistic algorithm.** As we have seen in Section 5, the computation of a basis of solutions of a system of linear equations is the most costly step of our algorithms. In IrreducibleDarbouxPolynomials, we have to consider four systems of linear equations. The first reason is that in IrreducibleDarbouxPolynomialsPartial, we need to study two linear systems in order to take into account the situation where $x = 0$ is a vertical tangent of the curve $M(x,y) = 0$. Indeed, in this situation we can not get a parametrization $\big(x, y(x)\big)$ of the curve. The second reason is that we need to use a change of coordinates in order to control the situation where $M(0,y)$ has a root at infinity. Of course, for a generic polynomial vector field, these two situations (i.e., a vertical tangent and a root at infinity) do not appear. We then deduce the following probabilistic algorithm.

Algorithm ProbabilisticIrreducibleDarbouxPolynomials

`Input:` A, $B \in \mathbb{K}[x,y]$, a bound $N \in \mathbb{N}$ such that (S) has no rational first integral of degree at most N, and two elements x_0, $\alpha \in \mathbb{K}$.
`Output:` The set of all irreducible Darboux polynomials M for the derivation $\mathcal{D}$ such that of $\deg(M) \leq N$.

(1) $\mathcal{E} := \emptyset$.
(2) Set $A_\alpha(x,y) = A(x + \alpha\, y, y) - \alpha\, B(x + \alpha\, y, y)$, $B_\alpha(x,y) = B(x + \alpha\, y, y)$ and $\mathcal{D}_\alpha = A_\alpha(x,y)\, \frac{\partial}{\partial x} + B_\alpha(x,y)\, \frac{\partial}{\partial y}$.

(3) For an indeterminate c, compute the polynomial $y_c \in \mathbb{K}(c)[x]$ of degree $\leq (N^2+1)$ s.t. $y_c(x_0) = c$ and $\frac{dy_c}{dx} \equiv \frac{B_\alpha(x,y_c)}{A_\alpha(x,y_c)} \mod x^{N^2+1}$.
(4) Let $M(x,y) = \sum_{i=0}^{N} \left(\sum_{j=0}^{N-i} m_{i,j}\, x^j\right) y^i$ be an ansatz for the Darboux polynomials that we are searching for.
(5) Construct the linear system $\mathcal{L}(c)$ for the $m_{i,j}$'s given by:
$$M(x, y_c(c,x)) \equiv 0 \mod x^{N^2+1}.$$
(6) Clear the denominator in $\mathcal{L}(c)$.
(7) Compute the Smith normal form of $\mathcal{L}(c)$. Let $\mathcal{P}(c)$ be the last invariant factor of $\mathcal{L}(c)$.
(8) Factorize $\mathcal{P}(c)$ over $\mathbb{K}$: $\mathcal{P}(c) = \prod_{i=1}^{s} \mathcal{P}_i(c)$.
  (a) For i from 1 to s do:
    (i) Set $\mathbb{K}[c_i] = \mathbb{K}[c]/(\mathcal{P}_i(c))$.
    (ii) Compute a solution of $\mathcal{L}(c_i)$ s.t. the corresponding polynomial M_i has minimal degree in y and is primitive w.r.t. y.
    (iii) If $\gcd(\mathcal{D}_\alpha(M_i), M_i) = M_i$, then $\mathcal{E} := \mathcal{E} \cup \{[M_i(c, x-\alpha\, y, y), \mathcal{P}_i(c)]\}$.
(9) Factorize $A_\alpha(x,0)$ over $\mathbb{K}$: $A_\alpha(x,0) = \prod_{i=1}^{k} A_i(x)$.
(10) For i from 1 to k do:
  (a) If $\gcd(\mathcal{D}_\alpha(A_i), A_i) = A_i$, then $\mathcal{E} := \mathcal{E} \cup \{[A_i(x - \alpha\, y, y), c-1]\}$.
(11) Return $\mathcal{E}$.

Proposition 33. *The algorithm ProbabilisticIrreducibleDarbouxPolynomials is correct. Furthermore, if x_0 and α are chosen uniformly at random in a finite set $\Omega \subset \mathbb{K}$ such that $|\Omega| > N d\,(\mathcal{B}(d)+1)$, then the probability that this algorithm returns all irreducible Darboux polynomials is at least* $\left(1 - \frac{N\,(\mathcal{B}(d)+1)}{|\Omega|}\right)\left(1 - \frac{N\,d\,(\mathcal{B}(d)+1)}{|\Omega|}\right)$.

Proof. First, we remark that M is a Darboux polynomial for $\mathcal{D}$ if and only if $M_\alpha(x,y) = M(x+\alpha y, y)$ is a Darboux polynomial for $\mathcal{D}_\alpha$. Thus the strategy used in this algorithm is to perform a change of coordinates in order to be in a generic position, and then to compute all irreducible Darboux polynomials M_α of degree at most N by considering only one linear system.
The proof of Proposition 30 shows that from Step (2) to Step (8), we compute all irreducible Darboux polynomials satisfying:
$$M_\alpha(x_0, y) \notin \mathbb{K} \quad \text{and} \quad \mathrm{Res}_y(M_\alpha(x_0,y), A_\alpha(x_0,y)) \neq 0.$$
Let us study the probability to get $M_\alpha(x_0,y) \notin \mathbb{K}$. If $M(x,y) = \sum_{0\leq i+j\leq N} a_{i,j}\, x^i\, y^j$, then $M_\alpha(x_0,y) = \left(\sum_{i+j=N} a_{i,j}\, \alpha^i\right) y^N + \cdots$ where the other terms have degree relatively to y strictly less than N. Thus, if $\sum_{i+j=N} a_{i,j}\alpha^i$ is not equal to zero, then we have $M_\alpha(x_0,y) \notin \mathbb{K}$.
As (S) has no rational first integral of degree at most N, then by Darboux-Jouanolou's theorem (see Theorem 6), we have at most $\mathcal{B}(d)+1$ irreducible Darboux polynomials with degree at most N. Thus, by Zippel-Schwartz's lemma, the probability to reach the situation $M_\alpha(x_0,y) \notin \mathbb{K}$ for all irreducible Darboux polynomials is at least $1 - (\mathcal{B}(d)+1)\, N/|\Omega|$.
Now we suppose that $M_\alpha(x_0,y) \notin \mathbb{K}$ and we study the probability to have the situation $\mathrm{Res}_y(M(x_0,y), A(x_0,y)) \neq 0$. If the polynomial $\mathrm{Res}_y(M(x,y), A(x,y))$ is not zero, then, by Zippel-Schwartz's lemma, the probability to reach this situation

for all irreducible Darboux polynomials, is at least $1-(\mathcal{B}(d)+1)\,N\,d/|\Omega|$.
If the polynomial $\mathrm{Res}_y(M_\alpha(x,y),A_\alpha(x,y))$ is zero, then M_α and A_α have a common factor. As we suppose M_α irreducible, we deduce that M_α divides A_α. Thus M_α divides $B_\alpha\,\partial_y(M_\alpha)$. As A_α and B_α are coprime, we get that M_α divides $\partial_y(M_\alpha)$. This situation is possible only when $\deg_y(M_\alpha)=0$. This means $\mathrm{Res}_y(M_\alpha(x,y),A_\alpha(x,y))\equiv 0$ when $\deg_y(M_\alpha)=0$ and M_α divides $A_\alpha(x,0)$. We compute this kind of irreducible Darboux polynomials in Step (10) of the algorithm. In conclusion, the algorithm computes all irreducible Darboux polynomials of degree at most N with the announced probability estimate. □

7.3. **Implementation and example.** We have implemented the algorithm ProbabilisticIrreducibleDarbouxPolynomials in our package RationalFirstIntegrals[4]. Let us illustrate the purpose of this section on an interesting example.
Consider the vector field corresponding to the jacobian derivation associated with $f(x,y)=(y-x-1)\,(x-y^2)\,(x\,y-1)$, namely,

$$A(x,y):=-\frac{\partial f}{\partial y}(x,y)=-3\,x^2y^2+4\,xy^3+x^3-2\,x^2y-3\,xy^2+x^2+2\,xy-3\,y^2+x+2\,y,$$

$$B(x,y):=\frac{\partial f}{\partial x}(x,y)=2\,xy^3-y^4-3\,x^2y+2\,xy^2+y^3-2\,xy-y^2+2\,x-y+1.$$

By construction, it admits the rational first integral f of degree 4 and the Darboux polynomials $M_1(x,y)=y-x-1$, $M_2(x,y)=x-y^2$, $M_3(x,y)=x\,y-1$ of degree at most 2. Let us consider the computation of all irreducible Darboux polynomials of degree at most $N=2$.
The first Darboux polynomial M_1 satisfies $M_1(0,y)=y-1\notin\mathbb{K}$ and its root $c_{M_1}=1$ satisfies $A(0,c_{M_1})=-1\neq 0$. Therefore it will be found by considering the linear system $\mathcal{L}_1(c)$ in IrreducibleDarbouxPolynomialsPartial, see the proof of Proposition 30.
The Darboux polynomial M_2 satisfies $M_2(0,y)=-y^2\notin\mathbb{K}$ and but its root $c_{M_2}=0$ satisfies $A(0,c_{M_2})=0$. Thus it will be missed if we only consider system $\mathcal{L}_1(c)$ in IrreducibleDarbouxPolynomialsPartial. It is the case where the curve $M_2(x,y)=0$ has the vertical tangent $x=0$. However, if we consider the second system $\mathcal{L}_2(c)$ in IrreducibleDarbouxPolynomialsPartial, we will find this Darboux polynomial, see the proof of Proposition 30.
Finally M_3 satisfies $M_3(0,y)=-1\in\mathbb{K}$ so that $M_3(0,y)$ has a root at infinity. Considering only the systems $\mathcal{L}_1(c)$ and $\mathcal{L}_2(c)$ in IrreducibleDarbouxPolynomialsPartial will not be enough to find this Darboux polynomial. However, performing the change of coordinates as in IrreducibleDarbouxPolynomials and applying IrreducibleDarbouxPolynomialsPartial to $-y\,\tilde{A}+\tilde{B}$ and $-\tilde{A}\,z$ instead of A and B will provide this Darboux polynomial.
To summarize, applying IrreducibleDarbouxPolynomialsPartial to A and B, we get M_1 and M_2 but we miss M_3 but either applying IrreducibleDarbouxPolynomials or ProbabilisticIrreducibleDarbouxPolynomials we get the three Darboux polynomials. Note also that applying an algorithm similar to ProbabilisticIrreducibleDarbouxPolynomials but where we skip Step (2), i.e., we do not perform the generic change of coordinate, we would obtain only M_1 and miss both M_2 and M_3.
Our implementation of ProbabilisticIrreducibleDarbouxPolynomials requires computations in $\mathbb{K}(c)$ so that as for GenericRationalFirstIntegral it is not very efficient and

[4]It is available at http://www.ensil.unilim.fr/~cluzeau/RationalFirstIntegrals.html

can not be used in practice for examples with large degrees. To give an idea of timings[5], on the previous example, running ProbabilisticIrreducibleDarbouxPolynomials without the change of coordinates in Step (2), we obtain $\{M_1\}$ in 2.737 seconds but we miss M_2 and M_3 whereas running ProbabilisticIrreducibleDarbouxPolynomials, we get the complete set $\{M_1, M_2, M_3\}$ in 9.775 seconds.

References

[ACFG05] J. M. Aroca, J. Cano, R. Feng, and X. S. Gao. Algebraic general solutions of algebraic ordinary differential equations. In *ISSAC'05*, pages 29–36 (electronic). ACM, New York, 2005. 11

[AHS03] Shreeram S. Abhyankar, William J. Heinzer, and Avinash Sathaye. Translates of polynomials. In *A tribute to C. S. Seshadri (Chennai, 2002)*, Trends Math., pages 51–124. Birkhäuser, Basel, 2003. 7

[BC11] L. Busé and G. Chèze. On the total order of reducibility of a pencil of algebraic plane curves. *J. Algebra*, 341:256–278, 2011. 7

[BCN11] Laurent Busé, Guillaume Chèze, and Salah Najib. Noether forms for the study of non-composite rational functions and their spectrum. *Acta Arith.*, 147(3):217–231, 2011. 6

[BCO+07] A. Bostan, F. Chyzak, F. Ollivier, B. Salvy, É. Schost, and A. Sedoglavic. Fast computation of power series solutions of systems of differential equations. In *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1012–1021, New York, 2007. ACM. 17

[BCS+07] Alin Bostan, Frédéric Chyzak, Bruno Salvy, Grégoire Lecerf, and Éric Schost. Differential equations for algebraic functions. In *ISSAC 2007*, pages 25–32. ACM, New York, 2007. 11

[BK78] R. P. Brent and H. T. Kung. Fast algorithms for manipulating formal power series. *J. Assoc. Comput. Mach.*, 25(4):581–595, 1978. 9, 17

[BL94] Bernhard Beckermann and George Labahn. A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM J. Matrix Anal. Appl.*, 15(3):804–823, 1994. 19

[BLS+04] A. Bostan, G. Lecerf, B. Salvy, E. Schost, and B. Wiebelt. Complexity issues in bivariate polynomial factorization. In *Proceedings of ISSAC 2004*, pages 42–49. ACM, 2004. 8

[Bod08] Arnaud Bodin. Reducibility of rational functions in several variables. *Israel J. Math.*, 164:333–347, 2008. 7

[BP94] Dario Bini and Victor Y. Pan. *Polynomial and matrix computations. Vol. 1.* Progress in Theoretical Computer Science. Birkhäuser Boston Inc., Boston, MA, 1994. Fundamental algorithms. 17, 18

[Car94] Manuel M. Carnicer. The Poincaré problem in the nondicritical case. *Ann. of Math. (2)*, 140(2):289–294, 1994. 4

[CFL10] Bartomeu Coll, Antoni Ferragut, and Jaume Llibre. Polynomial inverse integrating factors for quadratic differential systems. *Nonlinear Anal.*, 73(4):881–914, 2010. 8

[CG06] Javier Chavarriga and Isaac A. García. The Poincaré problem in the non-resonant case: an algebraic approach. *Differ. Geom. Dyn. Syst.*, 8:54–68 (electronic), 2006. 4

[CGG05] J. Chavarriga, H. Giacomini, and M. Grau. Necessary conditions for the existence of invariant algebraic curves for planar polynomial systems. *Bull. Sci. Math.*, 129(2):99–126, 2005. 7, 8

[CGGL03] Javier Chavarriga, Hector Giacomini, Jaume Giné, and Jaume Llibre. Darboux integrability and the inverse integrating factor. *J. Differential Equations*, 194(1):116–139, 2003. 8

[Chè11] Guillaume Chèze. Computation of Darboux polynomials and rational first integrals with bounded degree in polynomial time. *J. Complexity*, 27(2):246–262, 2011. 1, 2, 7, 8, 15, 20

[Chè12a] Guillaume Chèze. Bounding the number of remarkable values via Jouanolou's theorem. Technical report, Institut de Mathématiques de Toulouse, 2012. 7

[5]All the computations were made on a 2.7 GHz Intel Core i7

[Chè12b] Guillaume Chèze. A recombination algorithm for the decomposition of multivariate rational functions. *Mathematics of Computation (to appear)*, 2012. 5

[CLN91] D. Cerveau and A. Lins Neto. Holomorphic foliations in $\mathbf{C}\mathrm{P}(2)$ having an invariant algebraic curve. *Ann. Inst. Fourier (Grenoble)*, 41(4):883–903, 1991. 4

[CMS06] S. C. Coutinho and L. Menasché Schechter. Algebraic solutions of holomorphic foliations: an algorithmic approach. *J. Symbolic Comput.*, 41(5):603–618, 2006. 7, 8

[CMS09] S. C. Coutinho and L. Menasché Schechter. Algebraic solutions of plane vector fields. *J. Pure Appl. Algebra*, 213(1):144–153, 2009. 7, 8

[Dar78] Gaston Darboux. Mémoire sur les équations diff'érentielles du premier ordre et du premier degré. *Bull. Sci. Math.*, 32:60–96, 123–144, 151–200, 1878. 1, 3, 4, 7

[DDdMS01] L. G. S. Duarte, S. E. S. Duarte, L. A. C. P. da Mota, and J. E. F. Skea. Solving second-order ordinary differential equations by extending the Prelle-Singer method. *J. Phys. A*, 34(14):3015–3024, 2001. 7, 8

[DLA06] Freddy Dumortier, Jaume Llibre, and Joan C. Artés. *Qualitative theory of planar differential systems*. Universitext. Springer-Verlag, Berlin, 2006. 4, 7

[FG10] Antoni Ferragut and Hector Giacomini. A new algorithm for finding rational first integrals of polynomial vector fields. *Qual. Theory Dyn. Syst.*, 9(1-2):89–99, 2010. 1, 7, 8, 9, 10, 11, 21, 22

[FL07] Antoni Ferragut and Jaume Llibre. On the remarkable values of the rational first integrals of polynomial vector fields. *J. Differential Equations*, 241(2):399–417, 2007. 5, 7

[gGG99] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999. 15, 17

[GL10] Jaume Giné and Jaume Llibre. On the integrable rational Abel differential equations. *Z. Angew. Math. Phys.*, 61(1):33–39, 2010. 23

[Gor01] Alain Goriely. *Integrability and nonintegrability of dynamical systems*, volume 19 of *Advanced Series in Nonlinear Dynamics*. World Scientific Publishing Co. Inc., River Edge, NJ, 2001. 7

[GRS02] Jaime Gutierrez, Rosario Rubio, and David Sevilla. On multivariate rational function decomposition. *J. Symbolic Comput.*, 33(5):545–562, 2002. Computer algebra (London, ON, 2001). 6

[Jou79] J. P. Jouanolou. *Équations de Pfaff algébriques*, volume 708 of *Lecture Notes in Mathematics*. Springer, Berlin, 1979. 4, 7

[Kal85] Erich Kaltofen. Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM J. Comput.*, 14(2):469–489, 1985. 11

[Lec06] G. Lecerf. Sharp precision in Hensel lifting for bivariate polynomial factorization. *Mathematics of Computation*, 75:921–933, 2006. 8

[Lor93] Dino Lorenzini. Reducibility of polynomials in two variables. *J. Algebra*, 156(1):65–75, 1993. 7

[LY05] Jinzhi Lei and Lijun Yang. Algebraic multiplicity and the Poincaré problem. In *Differential equations with symbolic computation*, Trends Math., pages 143–157. Birkhäuser, Basel, 2005. 4

[LZ10] Jaume Llibre and Xiang Zhang. Rational first integrals in the Darboux theory of integrability in $\mathbb{C}^n$. *Bull. Sci. Math.*, 134(2):189–195, 2010. 7

[MM97] Yiu-Kwong Man and Malcolm A. H. MacCallum. A rational approach to the Prelle-Singer algorithm. *J. Symbolic Comput.*, 24(1):31–43, 1997. 6, 7, 8

[MO04] Jean Moulin Ollagnier. Algebraic closure of a rational function. *Qual. Theory Dyn. Syst.*, 5(2):285–300, 2004. 5

[Olv93] Peter J. Olver. *Applications of Lie groups to differential equations*, volume 107 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993. 7

[Per01] Jorge Vitório Pereira. Vector fields, invariant varieties and linear systems. *Ann. Inst. Fourier (Grenoble)*, 51(5):1385–1405, 2001. 8

[Per02] Jorge Vitório Pereira. On the Poincaré problem for foliations of general type. *Math. Ann.*, 323(2):217–226, 2002. 4

[Poi91] Henri Poincaré. Sur l'intégration algébrique des équations différentielles du premier ordre et du premier degré. *Rend. Circ. Mat. Palermo*, 5:161–191, 1891. 4, 5, 7

[PS83] M. J. Prelle and M. F. Singer. Elementary first integrals of differential equations. *Trans. Amer. Math. Soc.*, 279(1):215–229, 1983. 1, 7, 8

[Rup86] Wolfgang Ruppert. Reduzibilität ebener Kurven. *J. Reine Angew. Math.*, 369:167–191, 1986. 7

[Sch93] Dana Schlomiuk. Elementary first integrals and algebraic invariant curves of differential equations. *Exposition. Math.*, 11(5):433–454, 1993. 7

[Sch00] A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier. 5, 6

[SGR90] Dana Schlomiuk, John Guckenheimer, and Richard Rand. Integrability of plane quadratic vector fields. *Exposition. Math.*, 8(1):3–25, 1990. 7

[Sha74] R. E. Shafer. On quadratic approximation. *SIAM J. Numer. Anal.*, 11:447–460, 1974. 19

[Sha78] Robert E. Shafer. On quadratic approximation. II. *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz.*, (602-633):163–170 (1979), 1978. 19

[Sin92] Michael F. Singer. Liouvillian first integrals of differential equations. *Trans. Amer. Math. Soc.*, 333(2):673–688, 1992. 3, 4, 7

[SZ94] Bruno Salvy and Paul Zimmermann. GFUN: a Maple package for the manipulation of generating and holonomic functions in one variable. *ACM Transactions on Mathematical Software*, 20(2):163–167, 1994. 19

[vHW05] Mark van Hoeij and Jacques-Arthur Weil. Solving second order differential equations with klein's theorem. In *ISSAC 2005 (Beijing)*. ACM, New York, 2005. 23

[Vis93a] Angelo Vistoli. Erratum: "The number of reducible hypersurfaces in a pencil". *Invent. Math.*, 113(2):445, 1993. 7

[Vis93b] Angelo Vistoli. The number of reducible hypersurfaces in a pencil. *Invent. Math.*, 112(2):247–262, 1993. 7

[Wal00] Sebastian Walcher. On the Poincaré problem. *J. Differential Equations*, 166(1):51–78, 2000. 4

[Wei95] Jacques-Arthur Weil. *Constantes et polynômes de Darboux en algèbre différentielle : applications aux systèmes différentiels linéaires*. PhD thesis, École polytechnique, 1995. 7, 10

Alin Bostan: INRIA Saclay Île-de-France, Bâtiment Alan Turing, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France

E-mail address: alin.bostan@inria.fr

Guillaume Chèze: Institut de Mathématiques de Toulouse, Université Paul Sabatier Toulouse 3, MIP Bât. 1R3, 31 062 TOULOUSE cedex 9, France

E-mail address: guillaume.cheze@math.univ-toulouse.fr

Thomas Cluzeau: Université de Limoges ; CNRS ; XLIM UMR 7252 ; DMI, 123 avenue Albert Thomas, 87 060 LIMOGES cedex, France

E-mail address: cluzeau@ensil.unilim.fr

Jacques-Arthur Weil: Université de Limoges ; CNRS ; XLIM UMR 7252 ; DMI, 123 avenue Albert Thomas, 87 060 LIMOGES cedex, France

E-mail address: jacques-arthur.weil@unilim.fr