ALGEBRAIC SOLUTIONS OF PLANE VECTOR FIELDS

S. C. COUTINHO AND L. MENASCHÉ SCHECHTER

To Alcides Lins Neto on his 60th birthday

ABSTRACT. We present an algorithm that can be used to check whether a given derivation of the complex affine plane has an invariant algebraic curve and discuss the performance of its implementation in the computer algebra system SINGULAR.

1. Introduction

In a paper published in 1878 [10], Darboux showed that the algebraic curves invariant under a polynomial vector field can be used to determine a first integral of the correspondent first order differential equation. A differential equation that can be integrated by this method is said to be *Darboux integrable*. Although Darboux's method was a standard topic of textbooks of the late 19th and early 20th centuries, such as [13, p. 29, §2.21] and [14, p. 30, §25–32], it had no place in the developments that took over the theory of differential equations for most of the last century. However, things did change with the advent of the computer. Indeed, the search for invariant algebraic curves plays an important role in the method developed by M. J. Prelle and M. F. Singer [22] in the 1980s in order to compute elementary first integrals of differential equations.

Even though the polynomial vector fields that appear in applications often have invariant algebraic curves, this is by no means the rule. Indeed, a *generic* vector field of degree greater than or equal to 2 (see section 2 for the definition) does not have any invariant algebraic curves. This result, first stated (with an incorrect proof) in [18, Lemma 4, p. 180], is proved in [1, theorem 5, p. 342] and [20, Theorem 3, p. 385].

However, it turns out that it is usually quite hard to determine whether an explicitly given vector field has invariant algebraic curves or not. This is not very satisfactory. For example, vector fields without invariant algebraic curves can be used in the construction of $\mathcal{D}$-modules with various properties, such as irreducible nonholonomic $\mathcal{D}$-modules, indecomposable $\mathcal{D}$-modules and GK-critical $\mathcal{D}$-modules; see [1, section 4.3, p. 236] and [8]. Taking into account how poorly understood these

---

Date: May 5, 2008.

1991 *Mathematics Subject Classification.* Primary: 13P10, 37F75; Secondary: 32S65, 34M45.

Key words and phrases. derivation, singularity, invariant curve.

We thank the referee of [9], who suggested that the methods of that paper might also be applicable to vector fields of the affine plane, and J. V. Pereira who pointed out that, using extactic curves, our algorithm could be greatly improved. The first author was partially supported by grants from CNPq and PRONEX(Commutative algebra and algebraic geometry), and the second author by a scholarship from CNPq.

$\mathcal{D}$-modules are, explicit examples are needed in order to explore their properties and propose conjectures.

Another area in which it is necessary to check whether a given vector field has invariant curves is the study of centres of systems of differential equations. For example, it has been conjectured by Żołądek that a system of real polynomial differential equations in dimension two has a centre if and only if it is integrable in the sense of Darboux, as explained above, or has an algebraic symmetry; see [5, Conjecture 1.2, p. 8]. Since a system without invariant curves cannot be Darboux integrable, an algorithmic test for the existence of invariant curves will be of help both in determining whether a given system has a centre and in settling Żołądek's conjecture. For more on the relation between the problem of the centre and invariant curves see [6].

This is precisely the problem we tackle in this paper: building on the ideas of [9] we present an algorithm that allows one to test a given vector field (with rational coefficients) for the existence of invariant algebraic curves. Although the algorithm may be unable to come to a conclusion (thus returning *the algorithm failed*) it is very efficient for vector fields defined by polynomials for which all coefficients are nonzero up to the top monomial of highest degree (often called *dense polynomials*). See section 5 for details.

The paper contains four sections, besides this introduction. In section 2, we recall a number of general results of the theory of holomorphic foliations that will be used in the sequel. Section 3 contains a study of the behaviour of an invariant algebraic curve at the points where its projectivization intersects the line at infinity of $\mathbb{P}^2(\mathbb{C})$. The behaviour of algebraic solutions at the singular points of the derivation is considered in section 4. This section also contains a description and proof of the algorithm, whose performance is discussed in section 5.

2. Preliminaries

The following notation and hypotheses will be in force throughout the paper. Let

$$D_{a,b} = a\frac{\partial}{\partial x} + b\frac{\partial}{\partial y}$$

be a derivation of $\mathbb{C}[x,y]$, where a and b are polynomials that satisfy:

H.1: $a, b \in \mathbb{Q}[x,y]$;
H.2: $\deg(a) = \deg(b) = n \geq 2$;
H.3: $ya_n - xb_n$ is nonzero and irreducible over $\mathbb{Q}$.

The derivation $D_{a,b}$ of $\mathbb{C}[x,y]$ gives rise to the 1-form $\omega_{a,b} = bdx - ady$ of $\mathbb{C}^2$. Denote by U_z the open subset of the complex projective plane $\mathbb{P}^2$ defined by $z \neq 0$, and let $\pi : U_z \to \mathbb{C}^2$ be the map defined by $\pi([x:y:z]) = (x/z, y/z)$. Set

$$\Omega_{a,b} = z^r \pi^*(bdx - ady), \tag{2.1}$$

where r is chosen so as to clear the poles of the pullback form. Since we are assuming that $\deg(a) = \deg(b) = n > 1$,

$$\Omega_{a,b} = zBdx - zAdy + (yA - xB)dz, \tag{2.2}$$

where A and B denote the homogenizations of a and b with respect to z. The 1-form $\Omega_{a,b}$ defines a foliation of $\mathbb{P}^2$ that we denote by $\mathcal{F}_{a,b}$. From now on we will drop the subscript unless we need to call attention to the dependency of D, Ω or $\mathcal{F}$

on the coefficients a and b. Under the above hypotheses, the *degree* of $\mathcal{F}$ is n. For the definition of the degree of a foliation of $\mathbb{P}^2$, see [4, p. 884].

A *singularity* $[x_0 : y_0 : z_0] \in \mathbb{P}^2$ of $\mathcal{F}$ is a common zero of the coefficients of Ω. By (2.2) this means that either

$$a(x_0, y_0) = b(x_0, y_0) = 0 \text{ or } \quad z_0 = y_0 a_n(x_0, y_0) - x_0 b_n(x_0, y_0) = 0.$$

As one easily checks, (H.3) implies that $\gcd(a, b) = 1$. In particular, by Bézout's Theorem, $\mathcal{F}$ has a finite set of singularities, which we will denote by $\mathrm{Sing}(\mathcal{F})$. We also use the notation $\mathrm{Sing}(D) = \mathrm{Sing}(\mathcal{F}) \cap U_z$.

Let $\overline{C}$ be a reduced curve in $\mathbb{P}^2$; that is $\overline{C}$ is the zero set $\mathcal{Z}(F)$ of a squarefree homogeneous polynomial $F(x, y, z) \in \mathbb{C}[x, y, z]$. We say that $\overline{C}$ is *invariant* under $\mathcal{F}$ if there exists a homogeneous 2-form Θ so that

$$\Omega \wedge dF = F\Theta. \tag{2.3}$$

An invariant curve that is irreducible is also called an *algebraic solution* of $\mathcal{F}$. Note that z is an invariant algebraic curve of Ω as an inspection of (2.2) shows. If $F \neq z$, then (2.3) is equivalent to

$$D(f) = gf \tag{2.4}$$

where $f(x, y) = F(x, y, 1)$ is the dehomogenization of F at U_z and $g \in \mathbb{C}[x, y]$. Conversely, if a squarefree polynomial $f \in \mathbb{C}[x, y]$ satisfies (2.4) then its homogenization F, with respect to z is an invariant algebraic curve of Ω. In this case we also say that f is *invariant* under Ω. Thus, a curve C of the affine plane $\mathbb{C}^2$ is invariant under D if and only if its projectivization $\overline{C} \subset \mathbb{P}^2$ is invariant under Ω.

Our first proposition states that if a 1-form Ω with rational coefficients has an invariant algebraic curve (with complex coefficients) then it must have one (not necessarily the same) with rational coefficients. For a proof of this well-known result see [19] or [9].

Proposition 2.1. *If Ω has an invariant algebraic curve besides the line at infinity L_∞, then there exists $F \in \mathbb{Q}[x, y, z]$, $F \neq z$, such that $\mathcal{Z}(F)$ is also an invariant algebraic curve of Ω.*

Thus, to prove that a 1-form Ω, with rational coefficients, does not have invariant algebraic curves in $\mathbb{P}^2 \setminus L_\infty$, it is enough to consider the special case in which the solution is defined by a polynomial of $\mathbb{Q}[x, y, z]$. Therefore, we may add the following hypothesis to the ones already made at the beginning of the section,

H.4: unless otherwise stated, all curves are defined over $\mathbb{Q}$.

Unlike the other hypotheses, that will be recalled whenever necessary, this one will be taken for granted from now on.

Lemma 2.2. *If $\overline{C}$ is a reduced invariant algebraic curve of $\mathcal{F}$, which does not have L_∞ as one of its irreducible components, then*

$$\emptyset \neq \overline{C} \cap L_\infty = \mathrm{Sing}(\mathcal{F}) \cap L_\infty$$

is a set of $n + 1$ elements.

Proof. Since both $\overline{C}$ and L_∞ are algebraic solutions of $\mathcal{F}$, so are their intersection points. Therefore,

$$\emptyset \neq \overline{C} \cap L_\infty \subseteq \mathrm{Sing}(\mathcal{F}).$$

Now, let $\overline{C} = \mathcal{Z}(F)$, for some homogeneous polynomial $F \in \mathbb{Q}[x, y, z]$. Thus, $F(x, y, 0)$ is a nonzero polynomial, and $\overline{C} \cap L_\infty$ is defined by $F(x, y, 0) = 0$. But the singularities of $\mathcal{F}$ in L_∞ are the roots of $ya_n - xb_n$. Thus, $\gcd(F(x, y, 0), ya_n - xb_n) \neq 1$. However, $ya_n - xb_n$ is irreducible over $\mathbb{Q}$ by H.3. Since $F(x, y, 0)$ also has rational coefficients, it follows that $ya_n - xb_n$ divides $F(x, y, 0)$. Hence, these polynomials have the same squarefree decomposition, which proves the equality of the statement. Moreover, since $ya_n - xb_n$ has degree $n + 1$, the set $\mathrm{Sing}(\mathcal{F}) \cap L_\infty$ has exactly $n + 1$ distinct singularities. □

The 1-jet of $\mathcal{F}$ at a point $p \in \mathrm{Sing}(\mathcal{F})$ is the matrix

$$J(p) = \begin{bmatrix} \partial a/\partial x & \partial a/\partial y \\ \partial b/\partial x & \partial b/\partial y \end{bmatrix}.$$

We say that $\mathcal{F}$ is *nondegenerate* at p if $\det(J(p)) \neq 0$. In this case, the eigenvalues λ_1 and λ_2 of $J(p)$ are both nonzero, and the quotient λ_1/λ_2 and its reciprocal are the *characteristic exponents* of $\mathcal{F}$ at p. Let $S \subset \mathrm{Sing}(\mathcal{F})$. The set of all complex numbers that are characteristic exponents of $\mathcal{F}$ at a singularity in S will be denoted by $\mathrm{Exp}_{\mathcal{F}}(S)$. The key result to most of our proofs is the following proposition.

Proposition 2.3. *Let $\overline{C} \neq L_\infty$ be a reduced algebraic curve that is invariant under $\mathcal{F}$. If*

$$\mathrm{Exp}_{\mathcal{F}}(\mathrm{Sing}(\mathcal{F}) \cap L_\infty) \cap \mathbb{Q} = \emptyset$$

then $\overline{C}$ is nonsingular at its points at infinity and $\deg(\overline{C}) = n + 1$.

Proof. Let $\overline{C} = \mathcal{Z}(F)$ for some squarefree homogeneous polynomial $F \in \mathbb{C}[x, y, z]$. Since $F \neq z$, the polynomial zF defines an invariant algebraic curve of $\mathcal{F}$. However, the hypothesis on the characteristic exponents implies that $\overline{C}$ and L_∞ are transversal to each other at their intersection points; see [24, Theorem 2.3, p. 58]. . Hence, the former is nonsingular at every point of $\overline{C} \cap L_\infty$. In particular, the intersection multiplicity of $\overline{C}$ and L_∞ at every point of intersection of these two curves is one. Therefore, by Bézout's Theorem and Lemma 2.2, $\deg(\overline{C}) = n + 1$. □

An important application of the characteristic exponents of $\mathcal{F}$ concerns the Camacho-Sad index of a vector field, which will be required in the proofs of section 3. However, the definition we give is not the most general; indeed, it is taylored to the setup of the proofs in this paper. Let p be a nondegenerate singularity of $\mathcal{F}$ and let λ_1 and λ_2 be the eigenvalues of the 1-jet of $\mathcal{F}$ at p. Assume that $\lambda_1/\lambda_2 \notin \mathbb{Q}$. If C is a germ of holomorphic curve, smooth at p, and invariant under $\mathcal{F}$, then the *Camacho-Sad (or CS) index* of C at p is

$$\mathrm{CS}_{\mathcal{F}}(C, p) = \frac{\lambda_1}{\lambda_2},$$

where the tangent vector to C at p is an eigenvector of λ_2 with respect to the 1-jet of $\mathcal{F}$ at p.

Theorem 2.4 (Camacho-Sad)**.** *Let $\overline{C}$ be a smooth algebraic curve of $\mathbb{P}^2$ invariant under $\mathcal{F}$. The sum of the CS-indices of $\overline{C}$ over all the singularities of $\mathcal{F}$ contained in $\overline{C}$ is equal to* $\deg(\overline{C})^2$.

For a proof of this theorem see [3], [23, Chapter V, pp. 151–156] or [2, pp. 35–40]. The next result was originally stated by G. Darboux in [10, p. 84]; see [23, Theorem 1.1, p. 150] for a proof.

Proposition 2.5. *A foliation $\mathcal{F}$, of degree n, of $\mathbb{P}^2$ has n^2+n+1 singularities, counted with multiplicity. Moreover, if the n^2+n+1 singularities are distinct, then they are all nondegenerate.*

We now turn to the inflection points of algebraic curves. The *extactic* curve corresponding to the derivation $D_{a,b}$ is the curve of $\mathbb{C}^2$ defined by the polynomial

$$\mathcal{E}_{a,b} = bD(a) - aD(b).$$

See [21] and [7] for more details and further applications of these curves. The term *extactic* has been coined by D. Eisenbud. The next result was pointed out to us by J. V. Pereira.

Proposition 2.6. *Let C be an invariant algebraic curve of $D_{a,b}$ defined by a nonconstant polynomial $f \in \mathbb{C}[x,y]$. If f is a factor of $\mathcal{E}_{a,b}$ then C is a union of lines.*

Before we proceed to the proof, let us recall some basic facts about inflection points of an algebraic curve. Let C be an algebraic curve of $\mathbb{C}^2$ defined by an irreducible nonconstant polynomial $f \in \mathbb{C}[x,y]$. A smooth point p of C is an *inflection point* if the intersection multiplicity of C with the tangent line to C at p is greater than 2. An elementary calculation shows that this condition is equivalent to the vanishing at p of the polynomial

$$h_f = f_{xx}f_y^2 - 2f_xf_yf_{xy} + f_x^2f_{yy},$$

where

$$f_x = \frac{\partial f}{\partial x}, \quad f_y = \frac{\partial f}{\partial y}, \quad f_{xy} = \frac{\partial^2 f}{\partial x \partial y}, \text{ and so on.}$$

Note that, for every $p \in C$, the polynomial h_f vanishes at p if and only if the Hessian of F vanishes at p; see [17, Lemma 9.5, p. 84] for example.

Proof. Since every factor of f is stable under $D = D_{a,b}$ and divides $\mathcal{E}_{a,b}$, we may assume, without loss of generality, that f is irreducible as a polynomial of $\mathbb{C}[x,y]$. Let p be a smooth point of C that is not a singular point of D. Since f is stable under D, it follows that

$$D(f)|_p = D^2(f)|_p = 0.$$

The first of these equalities gives

$$a(p)f_x(p) + b(p)f_y(p) = 0. \tag{2.5}$$

On the other hand,

$$D^2(f) = (D(a)f_x + D(b)f_y) + (aD(f_x) + bD(f_y)). \tag{2.6}$$

The hypotheses on p imply that $a(p) \neq 0$ or $b(p) \neq 0$. Assuming, without loss of generality, that $a(p) \neq 0$, and taking (2.5) into account, we conclude that

$$a(p)(D(a)f_x + D(b)f_y)|_p = -f_y(p)\mathcal{E}_{a,b}|_p,$$

which is zero because f divide $\mathcal{E}_{a,b}$. Therefore, (2.6) gives

$$0 = D^2(f)|_p = (aD(f_x) + bD(f_y))|_p.$$

Now, using (2.5) again, we obtain from the definition of h_f that

$$a(p)^2h_f(p) = f_y(p)^2(aD(f_x) + bD(f_y))|_p,$$

which we have already shown to be equal to zero. Thus, $h_f(p) = 0$. In particular, both f and h_f vanish at all the smooth points of C, that are not singular points of D. Since these points are infinite in number, it follows by Bézout's theorem that f and h_f have a common component. However, f is irreducible, so it must divide h_f. Thus, f is a line by [17, Theorem 9.7, p. 85]. □

Although we have stated our results for vector fields with coefficients over the rational numbers, the same results hold over more general subfields of the complex numbers, including fields of algebraic numbers. We chose to stick to the rational numbers as our base field mainly because this is the case that we have implemented and whose performance is analysed in section 5.

3. Singularities at infinity

We begin with a study of the singularities of $\mathcal{F}$ at infinity. Since x does not divide a_n by H.3, it follows that all singularities of Ω at $z = 0$ have nonzero x-coordinate; so they can be put in the form $[1 : y : 0]$. Therefore, by H.3 again, there are exactly $n+1$ distinct singularities of this form in $z = 0$. In the open set $x \neq 0$ the foliation $\mathcal{F}$ is generated by the vector field

$$(y\hat{a} - \hat{b})\frac{\partial}{\partial y} + z\hat{a}\frac{\partial}{\partial z}, \tag{3.1}$$

where

$$\hat{a} = A(1, y, z) \text{ and } \hat{b} = B(1, y, z).$$

Now

$$\hat{a}(y, 0) = a_n(1, y) \text{ and } \frac{\partial \hat{a}}{\partial y}(y, 0) = \frac{\partial a_n}{\partial y}(1, y),$$

and similar formulae hold for $\hat{b}$. Thus,

$$\frac{\partial(y\hat{a} - \hat{b})}{\partial y}(y, 0) = a_n(1, y) + y\frac{\partial a_n}{\partial y}(1, y) - \frac{\partial b_n}{\partial y}(1, y),$$

while

$$\frac{\partial(z\hat{a})}{\partial y}(y, 0) = 0 \text{ and } \frac{\partial(z\hat{a})}{\partial z}(y, 0) = a_n(1, y).$$

Therefore, the eigenvalues of the 1-jet of the vector field (3.1) at a singularity $[1 : y : 0]$ of Ω are equal to

$$a_n(1, y) + y\frac{\partial a_n}{\partial y}(1, y) - \frac{\partial b_n}{\partial y}(1, y) \text{ and } a_n(1, y). \tag{3.2}$$

These are polynomials in y only. Moreover, if

$$\phi(y) = ya_n(1, y) - b_n(1, y),$$

the first of the two polynomials in (3.2) is equal to the derivative $\phi' = d\phi/dy$. In particular, if for some singularity $[1 : y_0 : 0]$ of Ω, the ratio of these eigenvalues is a number r, then $\psi(y_0, r) = 0$, where

$$\psi(y, t) = \phi'(y) - ta_n(1, y).$$

Therefore, all such r are roots of the resultant

$$\rho_1(t) = \mathrm{res}_y(\phi, \psi),$$

which is a polynomial of degree $n+1$. Denote by $(-1)^{n+1-k}q_k$ the ratio of the coefficient of degree k by the leading coefficient of ρ_1. Thus q_n is the sum of the roots of ρ_1.

Proposition 3.1. *Let $\overline{C} \subset \mathbb{P}^2$ be an invariant algebraic curve of $\mathcal{F}$. If ρ_1 has no rational roots and*

$$\mathrm{Sing}(\mathcal{F}) \cap \overline{C} \subset L_\infty$$

then $q_n = (n+1)^2$.

Proof. Note that $a_n(1, y_0) \neq 0$ at all singularities $[1 : y_0 : 0]$ of $\mathcal{F}$ for, otherwise, a_n and b_n could not be co-prime. Now, since ρ_1 has no rational roots it follows that $\overline{C}$ is nonsingular at infinity by Proposition 2.3. Thus,

$$\mathrm{CS}_{\mathcal{F}}(\overline{C}, [1 : y_0 : 0]) = \frac{\phi'(y_0)}{a_n(1, y_0)},$$

for all roots y_0 of $\phi(y_0) = 0$. Applying Theorem 2.4, we conclude that

$$\sum_{\{y_0 : \phi(y_0)=0\}} \mathrm{CS}_{\mathcal{F}}(\overline{C}, [1 : y_0 : 0]) = \deg(\overline{C})^2.$$

But the left hand side corresponds to the sum of the roots of ρ_1, which is equal to q_n. Therefore, $q_n = \deg(\overline{C})^2 = (n+1)^2$ by Proposition 2.3. □

The following corollary is an immediate consequence of the proposition.

Corollary 3.2. *Let $\overline{C} \subset \mathbb{P}^2$ be an invariant algebraic curve of $\mathcal{F}$. If ρ_1 has no rational roots and $q_n \neq (n+1)^2$, then*

$$\mathrm{Sing}(\mathcal{F}) \cap \overline{C} \cap U_z \neq \emptyset.$$

4. Finite singularities

In this section we deal with the singularities of $\mathcal{F}$ that belong to the open set $z \neq 0$. The hypotheses on D remain in force. By hypothesis H.2

$$\rho_2 = \mathrm{res}_y(a, b) \in \mathbb{Q}[x]$$

has degree at most n^2. Assuming that ρ_2 is irreducible of degree exactly n^2 over $\mathbb{Q}$, it follows from the Shape Lemma [16, Theorem 3.7.25, p. 257] that the ideal (a, b) of $\mathbb{Q}[x, y]$ can also be generated by ρ_2 and by a polynomial of the form $y - g(x)$, where $g \in \mathbb{Q}[x]$. Thus the Galois group $\mathrm{Gal}(\rho_2, \mathbb{Q})$ acts transitively over the singularities of D by

$$\sigma \cdot (x_0, g(x_0)) = (\sigma(x_0), g(\sigma(x_0))),$$

for a root x_0 of ρ_2 and an automorphism $\sigma \in \mathrm{Gal}(\rho_2, \mathbb{Q})$.

The next proposition relates the singularities of D to its invariant algebraic curves with rational coefficients.

Proposition 4.1. *Let $f \in \mathbb{Q}[x, y]$ be an invariant algebraic curve of D, and let $C = \mathcal{Z}(f)$. If*

1. *ρ_1 has no rational roots;*
2. *$q_n \neq (n+1)^2$; and*
3. *ρ_2 is irreducible of degree n^2 over $\mathbb{Q}$;*

then C is a singular curve of $\mathbb{C}^2$, and

$$\mathrm{Sing}(D) = \mathrm{Sing}(C).$$

Proof. Suppose, first of all, that C is a nonsingular curve. By (1) and Proposition 2.3, the curve $\overline{C}$ is nonsingular at infinity, and has degree $n+1$. Now, by (1), (2), and Corollary 3.2 there exists a singularity $p \in \mathbb{P}^2 \setminus L_\infty$ of D such that $f(p) = 0$. Since f has rational coefficients it follows that $f(\sigma(p)) = 0$ for all $\sigma \in \mathrm{Gal}(\rho_2, \mathbb{Q})$. Moreover, $\mathrm{Gal}(\rho_2, \mathbb{Q})$ acts transitively in $\mathrm{Sing}(D)$. Therefore, every singularity of D is a zero of f. Hence,

$$\mathrm{Sing}(D) \subset C. \tag{4.1}$$

Thus, $\overline{C}$ is a nonsingular curve of $\mathbb{P}^2$ that contains $\mathrm{Sing}(\mathcal{F})$.

Hence, by [15, Proposition 4.1, p. 126] there exists a homogeneous polynomial H, and a homogeneous 1-form Θ such that

$$\Omega = HdF + F\Theta, \tag{4.2}$$

where F denotes the homogenization of f with respect to z. Taking into account that both F, and the coefficients of Ω, have degree $n+1$, we see that

$$n + 1 = deg(H) + deg(F) - 1 = deg(H) + n;$$

so that $\deg(H) = 1$.

On the other hand, by (4.2), the form HdF vanishes at every singularity p of Ω. But, $\overline{C}$ is a nonsingular curve, which implies that $dF(p) \neq 0$ at every $p \in \overline{C}$. Thus, $H(p) = 0$ for every $p \in \mathrm{Sing}(\Omega)$. However, all the singularities of $\mathcal{F}$ are also zeroes of zA. Since A has degree n, it follows by Bézout's Theorem that

$$n^2 + n + 1 \leq \deg(zA)\deg(H) = \deg(A) + 1 = n + 1,$$

a contradiction. Therefore, C must be singular at some point of $\mathrm{Sing}(\mathcal{F})$. In other words,

$$\nabla f(p) = 0 \text{ for some } \; p \in \mathrm{Sing}(D).$$

However, since $\mathrm{Gal}(\rho_2, \mathbb{Q})$ acts transitively on the set $\mathrm{Sing}(D)$, it follows that C must be singular at all the singularities of D, which proves the proposition. □

The key result of this section is the following theorem.

Theorem 4.2. *Assume that:*

(1) ρ_1 *has no rational roots;*
(2) $q_n \neq (n+1)^2$*;*
(3) ρ_2 *is irreducible of degree* n^2 *over* $\mathbb{Q}$*.*

If $f \in \mathbb{Q}[x, y] \setminus \mathbb{Q}$ *is an invariant algebraic curve of* D*, then* f *is a polynomial of degree* $n+1$ *that divides* $\mathcal{E}_{a,b} = bD(a) - aD(b)$*.*

Proof. Since ρ_2 is irreducible of degree n^2, it follows that $\mathcal{Z}(a)$ intersects $\mathcal{Z}(b)$ transversely in n^2 distinct points. Moreover, by (1), (2), and (3) and Proposition 4.1 all these points belong to $\mathcal{Z}(f)$. Since this holds for any invariant algebraic curve of D with rational coefficients, we may assume, without loss of generality, that f is irreducible over $\mathbb{Q}$. Therefore, by Noether's Theorem [11, chapter 5, section 5, Proposition 1],

$$F = G_1 A + G_2 B.$$

However, $\deg(F) = n + 1$ by Proposition 2.3 which implies that $\deg(G_i) = 1$ for $i = 1, 2$. Let

$$G_1 = \alpha_1 x + \alpha_2 y + \alpha_3 z \quad \text{and} \quad G_2 = \beta_1 x + \beta_2 y + \beta_3 z.$$

By H.2, (1), Lemma 2.2, and Proposition 2.3,

$$m = \#(\mathrm{Sing}(\mathcal{F}) \cap L_\infty) = n + 1 \geq 3.$$

Denoting by $p_j = [1 : y_j : 0]$, for $1 \leq j \leq m$, the singularities of $\mathcal{F}$ at infinity, we have by Lemma 2.2 that

$$0 = f(p_j) = (\alpha_1 + \alpha_2 y_j)A(1, y_j, 0) + (\beta_1 + \beta_2 y_j)B(1, y_j, 0),$$

so that

$$(\alpha_1 + \alpha_2 y_j)a_n(1, y_j) + (\beta_1 + \beta_2 y_j)b_n(1, y_j) = 0. \tag{4.3}$$

Since p_j is a singularity at infinity of $\mathcal{F}$, it follows that

$$b_n(1, y_j) - y_j a_n(1, y_j) = 0. \tag{4.4}$$

Therefore, (4.3) may be rewritten as

$$a_n(1, y_j)(\alpha_1 + (\alpha_2 + \beta_1)y_j + \beta_2 y_j^2) = 0.$$

However, $a_n(1, y_j) \neq 0$ by (4.4) and H.3. Hence,

$$\alpha_1 + (\alpha_2 + \beta_1)y_j + \beta_2 y_j^2 = 0$$

for $1 \leq j \leq m$. This is a system of linear equations in the variables $\alpha_1, (\alpha_2 + \beta_1)$ and β_2. Since $m \geq 3$, the matrix of this system contains the minor

$$\begin{bmatrix} 1 & y_1 & y_1^2 \\ 1 & y_2 & y_2^2 \\ 1 & y_3 & y_3^2 \end{bmatrix}$$

whose determinant is

$$(y_3 - y_1)(y_3 - y_2)(y_1 - y_2) \neq 0.$$

Therefore,

$$\alpha_1 = \alpha_2 + \beta_1 = \beta_2 = 0$$

and

$$F = (\alpha_2 y + \alpha_3 z)A + (-\alpha_2 x + \beta_3 z)B. \tag{4.5}$$

However, F cannot be divisible by z, which implies that $\alpha_2 \neq 0$. Dividing f by α_2, we may assume that $\alpha_2 = 1$. Dehomogenizing (4.5) with respect to z, we find that

$$f = (y + \alpha_3)a + (-x + \beta_3)b \tag{4.6}$$

is a solution of D. Since f, a and b have rational coefficients, and $\gcd(a, b) = 1$ by H.3, it follows that $\alpha_3, \beta_3 \in \mathbb{Q}$. A simple computation shows that

$$D(f) = (y + \alpha_3)D(a) + (-x + \beta_3)D(b),$$

which must be divisible by f. Multiplying this last equation by a, and taking $(y + \alpha_3)a$ from (4.6) into it, we get

$$aD(f) = (f + (x - \beta_3)b)D(a) - (x - \beta_3)aD(b).$$

Since $D(f)$ is a multiple of f, by hypothesis, we may conclude that f divides

$$(x - \beta_3)(bD(a) - aD(b)).$$

However, f is irreducible over $\mathbb{Q}$ of degree $n + 1 > 1$. In particular, f cannot divide $x - \beta_3$; so it must divide $bD(a) - aD(b)$, which completes the proof of the theorem. □

Corollary 4.3. *If*

(1) ρ_1 *has no rational roots;*
(2) $q_n \neq (n+1)^2$*;*
(3) ρ_2 *is irreducible of degree* n^2*.*

then D *has no invariant algebraic curves in* $\mathbb{C}^2$*.*

Proof. Let $f \in \mathbb{Q}[x,y] \setminus \mathbb{Q}$ be an invariant algebraic curve of $D = D_{a,b}$. It follows from Theorem 4.2 that f has degree $n+1$ and divides $\mathcal{E}_{a,b}$. Thus, by Proposition 2.6, f is a product of $n+1$ linear polynomials. These linear polynomials must be all distinct, because f is a squarefree polynomial, so they form a set Λ of $n+1$ elements. Moreover, two distinct polynomials of Λ cannot intersect at the same point at infinity by Proposition 2.3. So, any two lines of Λ must have an intersection in $\mathbb{C}^2$.

Since the absolute Galois group G of $\mathbb{Q}$ acts on $\mathrm{Sing}(D)$ as $\mathrm{Gal}(\rho_2, \mathbb{Q})$, its action on the singularities of D is transitive. Moreover, if $\sigma \in G$, then

$$\prod_{\lambda \in \Lambda} \lambda = f = f^\sigma = \prod_{\lambda \in \Lambda} \lambda^\sigma$$

so that σ also acts on the Λ.

The elements of Λ are invariant algebraic curves of D, so the intersection of any two of them must occur at a singularity of D. Assume that some $p \in \mathrm{Sing}(D)$ is at the intersection of exactly k of the of lines of Λ; say

$$\{p\} = \lambda_1 \cap \cdots \cap \lambda_k.$$

Thus,

$$\{\sigma(p)\} = \lambda_1^\sigma \cap \cdots \cap \lambda_k^\sigma,$$

for every $\sigma \in \mathrm{Sing}(D)$. Since the action of G on $\mathrm{Sing}(D)$ is transitive, it follows that the number of lines in Λ that intersect at a singularity of D is exactly k for all $p \in \mathrm{Sing}(D)$. Moreover, $k \geq 2$.

Now, fix a line $\lambda \in \Lambda$. Every

$$\lambda' \in \Lambda \setminus \{\lambda\}$$

intersects λ in exactly one point (which must be a singularity of D), so we can count the n elements of $\Lambda \setminus \{\lambda\}$ in terms of the points of $\lambda \cap \mathrm{Sing}(D)$. Indeed, if ℓ is the number of singularities of D that belong to λ, and taking into account that exactly k lines (including λ) go through each singularity, we find that $n = (k-1)\ell$. In particular, this implies that every line in Λ contains the same number of singularities of D, which we will continue to denote by ℓ.

On the other hand, each singularity of D belongs to exactly k lines. So, multiplying the number ℓ of singularities per line by the number $n+1$ of lines we are counting each one of the n^2 singularities k times. In other words,

$$kn^2 = \ell(n+1). \tag{4.7}$$

But, taking $n = (k-1)\ell$ into equation (4.7), we get

$$k(k-1)^2\ell = n+1;$$

which implies that $k-1$ and ℓ divide $\gcd(n, n+1) = 1$. Therefore,

$$n = (k-1)\ell = 1,$$

which contradicts hypothesis (H.2). □

The algorithm that results from this corollary simply checks that all the required hypotheses are satisfied. If they are, the derivation has no invariant algebraic curves by Corollary 4.3; otherwise, the algorithm fails.

Algorithm 4.4. *Given a derivation $D_{a,b}$ where $a, b \in \mathbb{Q}[x, y]$ are polynomials of degree $n \geq 1$, the algorithm returns one of two messages:* `the algorithm failed` *or* `there are no invariant algebraic curves`*.*

Step 1: *If* $\deg(a) = \deg(b)$*, let* $n = \deg(a)$*; otherwise stop and return* `the algorithm failed`*.*
Step 2: *If* $n = 1$*, stop and return* `the algorithm failed`*.*
Step 3: *If the polynomial* $ya_n - xb_n$ *is zero or reducible, stop and return* `the algorithm failed`*.*
Step 4: *Set*

$$\phi(y) = ya_n(1, y) - b_n(1, y) \quad \text{and} \quad \psi(y, t) = \phi'(y) - ta_n(1, y)$$

and compute $\rho_1(t) = \mathrm{res}_y(\phi, \psi)$*.*
Step 5: *If* ρ_1 *has rational roots stop and return* `the algorithm failed`*.*
Step 6: *Denote by* $(-1)^{n+1-k} q_k$ *the ratio of the coefficient of degree* k *by the leading coefficient of* ρ_1*. If* $q_n = (n + 1)^2$*, stop and return* `the algorithm failed`*.*
Step 7: *Compute* $\rho_2 = res_y(a, b)$*.*
Step 8: *If* $\deg(\rho_2) < n^2$ *or* ρ_2 *is reducible over* $\mathbb{Q}$*, stop and return* `the algorithm failed`*; otherwise, stop and return* `there are no invariant algebraic curves`*.*

5. Experimental tests

The algorithm described in section 4 was implemented using the computer algebra system SINGULAR (version 2.0.5) [12]. All the tests discussed in this section were performed under Windows XP running on a micro-computer with an Intel Pentium 4 HT processor of 2.8 GHz, with 512 MB of primary memory.

The first test we performed calculated the average time taken by the algorithm to show that a generic derivation of a given degree, defined by a pair of randomly chosen dense polynomials does not have an invariant algebraic curve. Recall that a polynomial is dense if almost all of its coefficients are nonzero up to the top monomial of highest degree. Table 1 summarizes the output of a program that randomly generates 100 pairs of dense polynomials for each degree and computes the average CPU time taken to check that the derivation defined by each of the pairs does not have an invariant algebraic curve. In this first test, none of the derivations tested caused the algorithm to fail. This is not unexpected, because these derivations were defined by dense polynomials, with random coefficients, which makes them 'generic' in an experimental sense.

For higher degrees, the time taken to test 100 derivations with the algorithm starts to get too long. So, in order to have some results for derivations of degree higher than 19, we performed a second test, similar to the first, except that one derivation is tested for each degree. The CPU time taken by the algorithm to check that such a derivation does not have an invariant algebraic curve is shown in Table 2. Just as in the first test, no derivation caused the algorithm to fail.

Degree	2	3	4	5	6	7
Time	6	11	13	23	37	69
Degree	8	9	10	11	12	13
Time	117	234	395	700	1260	2171
Degree	14	15	16	17	18	19
Time	4796	7743	11027	17313	25824	37638

Table 1. Average execution time in ms of the algorithm for derivations defined by dense polynomials (100 derivations for each degree)

Degree	20	21	22	23	24	25
Time	56198	65625	96360	139593	200907	300500

Table 2. Execution time in ms of the algorithm for derivations defined by dense polynomials (1 derivation for each degree)

In the third test, we generated derivations defined by sparse polynomials. In this case, the algorithm fails rather often. As one might expect, the number of derivations for which the algorithm fails is proportional to the number of vanishing coefficients of the corresponding polynomials, as shown in Table 3. The data were obtained with a procedure that tests 100 randomly generated derivations of degree 4 for each type. In performing this test we used the Singular function `sparsepoly` which randomly chooses both the coefficients that are going to be zero and the size of the nonzero coefficients. This function also allows the user to choose the percentage of vanishing coefficients in the polynomial that it will generate. The dense polynomials used in the previous tests were obtained with the help of the same function, by setting this percentage to zero. See [12] for more details about this function.

As the tests show, the algorithm has an excellent success rate for what we might call "experimentally generic derivations"; that is, derivations that are defined by dense polynomials with random coefficients.

References

1. J. Bernstein and V. Lunts, *On non-holonomic irreducible D-modules*, Invent. Math. **94** (1988), 223–243.
2. M. Brunella, *Birational geometry of foliations*, 2004, pp. iv+138.
3. César Camacho and Paulo Sad, *Invariant varieties through singularities of holomorphic vector fields*, Ann. of Math. (2) **115** (1982), no. 3, 579–595.
4. D. Cerveau and A. Lins Neto, *Holomorphic foliations in* **CP**(2) *having an invariant algebraic curve*, Ann. Sc. de l'Institute Fourier **41** (1991), 883–903.
5. C. Christopher and Chengzhi Li, *Limit cycles of differential equations*, Advanced Courses in Mathematics, CRM, Barcelona, Birkhäuser, Basel, 2007.
6. C. J. Christopher, *Invariant algebraic curves and conditions for a centre*, Proc. Roy. Soc. Edinburgh Sect. A **124** (1994), no. 6, 1209–1229.

Percentage of coefficients equal to zero	Percentage of failures
0%	0%
20%	35%
30%	63%
50%	79%
70%	99%
80%	100%
90%	100%

Table 3. Percentage of derivations of degree 4 that cause the algorithm to fail for different percentages of vanishing coefficients (100 derivations for each percentage)

7. Colin Christopher, Jaume Llibre, and Jorge Vitório Pereira, *Multiplicity of invariant algebraic curves in polynomial vector fields*, Pacific J. Math. **229** (2007), no. 1, 63–117.
8. S. C. Coutinho, *Indecomposable non-holonomic* $\mathcal{D}$*-modules in dimension* 2, Proc. Edinburgh Math. Soc. **46** (2003), 341–355.
9. S. C. Coutinho and L. Menasché Schechter, *Algebraic solutions of holomorphic foliations: an algorithmic approach*, Journal of Symbolic Computation **41** (2006), 603–618.
10. G. Darboux, *Mémoire sur les équations différentielles algébriques du* I° *ordre et du premier degré*, Bull. des Sc. Math. (Mélanges) (1878), 60–96, 123–144, 151–200.
11. W. Fulton, *Algebraic curves: an introduction to algebraic geometry*, W. A. Benjamin, 1969.
12. G.-M. Greuel, G. Pfister, and H. Schönemann, *Singular version 1.2 user manual*, In *Reports On Computer Algebra* 21, Centre for Algebra, University of Kaiserslautern, 1998.
13. E. L. Ince, *Ordinary differential equations*, Dover, New York, 1956, first edition published in 1926.
14. C. Jordan, *Cours d'analyse de l'École Polytechnic*, third ed., vol. III, Gauthier-Villars, Paris, 1915.
15. J. P. Jouanolou, *Equations de Pfaff algébriques*, Lect. Notes in Math., vol. 708, Springer-Verlag, Heidelberg, 1979.
16. Martin Kreuzer and Lorenzo Robbiano, *Computational commutative algebra. 1*, Springer-Verlag, Berlin, 2000.
17. Ernst Kunz, *Introduction to plane algebraic curves*, Birkhäuser Boston Inc., Boston, MA, 2005, Translated from the 1991 German edition by Richard G. Belshoff.
18. E. M. Landis and I. G. Petrovskĭ, *On the number of limit cycles of the equation* $\frac{dy}{dx} = \frac{P(x,y)}{Q(x,y)}$ *where p and q are polynomials of the second degree*, Amer. Math. Soc. Transl. **10** (1958), 177–221.
19. Y.-K. Man and M. A. H. MacCallum, *A rational approach to the Prelle-Singer algorithm*, J. Symb. Computation **24** (1997), 31–43.
20. A. Lins Neto, P. Sad, and B. Scárdua, *On topological rigidity of projective foliations*, Bull. Soc. math. France **126** (1998), 381–406.
21. J. V. Pereira, *Vector fields, invariant varieties and linear systems*, Ann. Inst. Fourier (Grenoble) **51** (2001), no. 5, 1385–1405.
22. M. J. Prelle and M. F. Singer, *Elementary first integrals of differential equations*, Trans. Amer. Math. Soc. **279** (1983), 215–229.
23. T. Suwa, *Indices of vector fields and residues of singular holomorphic foliations*, Actualités Mathématiques, Hermann, Paris, 1998.
24. S. Walcher, *On the Poincaré problem*, J. Diff. Equations **166** (2000), 51–78.

Departamento de Ciência da Computação, Instituto de Matemática, Universidade Federal do Rio de Janeiro, P.O. Box 68530, 21945-970 Rio de Janeiro, RJ, Brazil.

Programa de Engenharia de Sistemas e Computação, COPPE, UFRJ, PO Box 68511, 21941-972, Rio de Janeiro, RJ, Brazil.
E-mail address: collier@impa.br
URL: http://www.dcc.ufrj.br/~collier

Programa de Engenharia de Sistemas e Computação, COPPE, UFRJ, PO Box 68511, 21941-972, Rio de Janeiro, RJ, Brazil.
E-mail address: luis@cos.ufrj.br