ANNALES

DE

L'INSTITUT FOURIER

S. C. COUTINHO

A constructive proof of the Density of Algebraic Pfaff Equations without Algebraic Solutions

Tome 57, n° 5 (2007), p. 1611-1621.

<http://aif.cedram.org/item?id=AIF_2007__57_5_1611_0>

Ann. Inst. Fourier, Grenoble
57, 5 (2007) 1611-1621

A CONSTRUCTIVE PROOF OF THE DENSITY OF ALGEBRAIC PFAFF EQUATIONS WITHOUT ALGEBRAIC SOLUTIONS

by **S. C. COUTINHO (*)**

Abstract. — We present a constructive proof of the fact that the set of algebraic Pfaff equations without algebraic solutions over the complex projective plane is dense in the set of all algebraic Pfaff equations of a given degree.

Résumé. — Nous présentons une preuve constructive du fait que l'ensemble des équations de Pfaff sans solutions algébriques sur le plan projectif complexe est dense dans l'ensemble de toutes les équations algébriques de Pfaff d'un degré donné.

1. Introduction

The computation of first integrals is an important topic in the theory of ordinary differential equations, and also in its applications to mechanics and physics. Various methods have been devised to compute such integrals. Of these, the one introduced by G. Darboux [7] in 1870, for equations of the first order and the first degree, in dimension two, has proved particularly effective. Indeed, as Prelle and Singer showed in [13], this leads to a procedure that can be used to compute elementary first integrals for such equations. The key to Darboux's method is the existence of a large enough set of algebraic curves invariant under the equation one wishes to solve.

Unfortunately, as Jouanolou showed in [8, Théorème 1.1, p. 158], first order equations of degree $n \geqslant 2$ rarely have any invariant curves whatsoever.

Keywords: Pfaff equation, singularity, algebraic solution.
Math. classification: Primary: 11R04, 37F75, 34M45; Secondary: 32S65.
(*) I wish to thank the referee for many comments that greatly improved the presentation of the paper. During the preparation of this paper I was partially supported by grants from CNPq and Pronex (commutative algebra and algebraic geometry).

Jouanolou's result can be easily stated in the language Pfaff equations, as follows. Let $\mathcal{P}_n$ be the vector space of algebraic Pfaff forms of degree n over the complex projective plane $\mathbb{P}^2$. Since two Pfaff forms that differ by a nonzero constant multiple define the same equation, the set of Pfaff equations can be identified with $\mathbb{P}(\mathcal{P}_n)$.

THEOREM 1.1. — *The set of algebraic Pfaff equations of degree $n \geqslant 2$ over $\mathbb{P}^2$ that do not have an algebraic solution is dense in $\mathbb{P}(\mathcal{P}_n)$.*

For the definition of the degree of a Pfaff equation see section 2. Jouanolou's proof of this result has two parts. First, he uses basic geometry of projective varieties to show that the set of Pfaff equations without algebraic solutions is either empty or dense in $\mathbb{P}(\mathcal{P}_n)$. Then he gives an explicit example of an equation without algebraic solutions. The hardest part of the proof consists in showing that the given equation does not have any algebraic solutions. Since then, several different proofs of the same result have appeared, for example [2, Theorem, p. 900], [11, section 3.2, p. 224], [10] and [12].

In this paper we present a new, constructive proof, of Theorem 1.1. By that we mean a proof that allows one to construct an explicit example of an equation without algebraic solutions in any neighbourhood of $\mathcal{P}_n$. Indeed, given such a neighbourhood, we construct an example of a Pfaff equation with coefficients in the field of gaussian numbers, that does not have any algebraic solutions. The construction is explicit and can be implemented as an algorithm. Our approach is arithmetical, and the equations we construct are very similar to Jouanolou's example when reduced modulo a certain prime.

2. Pfaff equations over the projective plane

In this section we discuss some basic facts about Pfaff equations over the projective plane $\mathbb{P}^2 = \mathbb{P}^2(\mathbb{C})$. Let $n \geqslant 0$ be an integer, and denote by x, y and z the homogeneous coordinates of the projective plane $\mathbb{P}^2$. A *Pfaff form* of $\mathbb{P}^2$ is a 1-form $\Omega = Adx + Bdy + Cdz$, where A, B and C are nonzero homogeneous polynomials of degree $n+1$ that satisfy the identity $xA+yB+zC = 0$. A *Pfaff equation* is an equivalence class of nonzero Pfaff forms modulo multiplication by nonzero constants. A *singularity* of Ω is a common zero of A, B and C. We denote the set of singularities of Ω by $\mathrm{Sing}(\Omega)$. If $\mathrm{Sing}(\Omega)$ is finite then Ω is *saturated*.

A nonconstant homogeneous polynomial $F \in \mathbb{C}[x,y,z]$ is an *algebraic solution* of Ω if there exists a 2-form Θ such that

$$\Omega \wedge dF = F\Theta. \tag{2.1}$$

In this case we also say that the curve $C = \mathcal{Z}(F) \subset \mathbb{P}^2$ is *invariant* under Ω.

Let U_z be the open set of $\mathbb{P}^2$ defined by $z \neq 0$ and let ω be the dehomogenization of Ω with respect to z. If $\pi_z : U_z \to \mathbb{C}^2$ is the map given by $\pi_z[x : y : z] = (x/z, y/z)$, then $\Omega = z^k \pi_z^*(\omega)$, where k is chosen so as to clear the poles of $\pi_z^*(\omega)$. Moreover, if f is the dehomogenization of a homogeneous polynomial $F \in \mathbb{C}[x,y,z]$, and assuming that F is not a constant multiple of a power of z, then F is an algebraic solution of Ω if and only if

$$\omega \wedge df = f\theta, \tag{2.2}$$

where θ is the dehomogenization of Θ. An f that satisfies (2.2) is also called an *algebraic solution* of ω. Thus, if our aim is to study algebraic solutions, we can switch between Pfaff forms over $\mathbb{P}^2$ and 1-forms over $U_z \cong \mathbb{C}^2$.

For reasons that will become clear later it is preferable to state our results in terms of 1-forms over $\mathbb{C}^2$. Thus, let $\omega = a\,dx + b\,dy$, where $a, b \in \mathbb{C}[x,y]$. Note that if Ω is as above, then

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

It follows from the relation $xA + yB + zC = 0$, that

$$a = yh + a_0 \text{ and } b = -xh + b_0, \tag{2.3}$$

where h is a homogeneous polynomial of degree n, and a_0 and b_0 are polynomials of degree at most n. The number n is called the *degree* of ω, and also of Ω. Note that, if $h \neq 0$, then

$$n = \deg(a) - 1 = \deg(b) - 1.$$

Consider now the space $\mathcal{P}_n$ of Pfaff forms of degree n, which corresponds to the nonzero triples (A,B,C) of homogeneous polynomials of degree $n+1$ that satisfy the identity $xA + yB + zC = 0$. It follows from the discussion above that $\mathcal{P}_n$ can be identified with the set of nonzero (h, a_0, b_0) where h is homogenous of degree n and a_0 and b_0 are polynomials of degree at most n. Thus, $\mathcal{P}_n \cup \{0\}$ is isomorphic to the affine $\mathbb{C}$-space of dimension $(n+1)(n+3)$.

The question whether h is zero or nonzero is quite significant for us, because if it is zero the line at infinity is invariant under Ω. Therefore, in this case, the Pfaff form always has an algebraic solution. This explains why we always assume that $h \neq 0$. Note, however, that any Pfaff form of $\mathcal{P}_n$ can be easily approximated by one with $h \neq 0$.

For our purposes it is more convenient to think of the elements of $\mathcal{P}_n$ as corresponding to 1-forms $\omega = adx + bdy$, such that a and b are given by (2.3). In particular, if ω is a generic element of $\mathcal{P}_n$ then $\gcd(a, b) = 1$; so that its homogenization Ω is saturated. A *singularity* of ω is a common zero of a and b. The set of all the singularities of ω is denoted by $\mathrm{Sing}(\omega)$. Because we are assuming that ω is saturated, it follows from Bézout's theorem that this is a finite set. Although, $\mathrm{Sing}(\omega)$ need not be equal to $\mathrm{Sing}(\Omega)$, the two sets coincide if $\mathrm{Sing}(\Omega)$ has empty intersection with the line at infinity L_∞. Indeed, in this case, every zero of A and B is also a zero of C because $xA + yB + zC = 0$. From now on, we assume that the coordinates of $\mathbb{P}^2$ have been chosen so that $\mathrm{Sing}(\Omega) \cap L_\infty = \emptyset$ for the Pfaff form Ω that is under consideration.

The following result was first stated and proved (for Pfaff equations over $\mathbb{Q}$) in [4, Theorem 3.1]. Since our main construction is based on it, we include a sketch of its proof. As usual, the ring of gaussian integers will be denoted by $\mathbb{Z}[i]$ and its quotient ring by $\mathbb{Q}[i]$.

THEOREM 2.1. — *Let a_0, b_0 be polynomials of degree at most n in $\mathbb{Q}[i][x, y]$. Suppose that $h \in \mathbb{Q}[i][x, y]$ is a nonzero homogeneous polynomial of degree n, and write*

$$a = hy + a_0 \quad \text{and} \quad b = -hx + b_0.$$

If the ideal $(a, b) \cap \mathbb{Q}[i][x]$ is generated by a polynomial of degree $n^2 + n + 1$ that is irreducible over $\mathbb{Q}[i]$, then $\omega = adx + bdy$ does not have any algebraic solutions in $\mathbb{P}^2$.

Proof. — Since we are assuming that $(a, b) \cap \mathbb{Q}[i][x]$ is generated by a polynomial of degree $n^2 + n + 1$, irreducible over $\mathbb{Q}[i]$, it follows that the polynomial of $\mathbb{Q}[i][x]$ whose roots are the x-coordinates of the points in $\mathrm{Sing}(\omega)$ is irreducible of degree $n^2 + n + 1$ over $\mathbb{Q}[i]$. However, the Pfaff form Ω, obtained by homogenizing ω, has at most $n^2 + n + 1$ singularities on $\mathbb{P}^2$. Therefore, all the singularities of Ω lie in $\mathbb{C}^2$ and have multiplicity one.

The hypothesis also implies that the absolute Galois group G of $\mathbb{Q}[i]$ acts transitively on the first coordinates of the singularities of ω. Hence, it also acts transitively on the singularities themselves. Thus, by the Baum-Bott Theorem, the eigenvalues of the 1-jets of ω at each one of its singularities, have an irrational ratio. This implies that a singular point of an algebraic solution of ω must be a node.

Now consider an algebraic curve $C \subset \mathbb{C}^2$ invariant under ω. The absolute Galois group G acts on C and leaves ω invariant. In particular, the image

C^σ of C under σ is also an algebraic curve invariant under ω. Thus, if C is not defined over a finite extension of $\mathbb{Q}[i]$, then ω has infinitely many algebraic invariant curves; hence it has a first integral by [8, Théorème 3.3, p. 102]. Since this integral is defined over $\mathbb{Q}[i]$, we have obtained an invariant curve with coefficients in $\mathbb{Q}[i]$. Otherwise, C is defined over a finite algebraic extension of $\mathbb{Q}[i]$. Hence, there are only finitely many C^σ, for $\sigma \in G$, and their union is an invariant algebraic curve of ω with coefficients in $\mathbb{Q}[i]$. Whatever the case, we end up with an algebraic curve defined over $\mathbb{Q}[i]$ and invariant under ω. Therefore, from now on, we may assume that C itself is defined over $\mathbb{Q}[i]$.

By [8, Proposition 4.1, p. 126], C must contain, at least, one singularity of ω. But G acts transitively on $\mathrm{Sing}(\omega)$ and stabilizes C; so it must contain all the singularities of ω. Moreover, since the separatrices of ω are smooth and transversal at all of its singular points, it follows that C is either a smooth curve, or a singular curve with n^2+n+1 nodes. We must show that both these cases lead to a contradiction.

Let d be the degree of the curve C. If C is smooth, then by [1, Proposition 4, p. 532],

$$d(n+2) = d^2 + n^2 + n + 1,$$

which is not possible. Otherwise, C has n^2+n+1 nodes, so that, $d = n+2$ by [1, Proposition 4, p. 532 and Proposition 7, p. 536]. However, by Bézout's Theorem,

$$d(d-1) \geqslant \sum_{p \in \mathrm{Sing}(C)} m_p(m_p - 1), \tag{2.4}$$

where m_p is the multiplicity of C at the singular point p. Since the curve is nodal, $m_p = 2$. Taking this into (2.4), together with $d = n+2$, we find that

$$(n+2)(n+1) \geqslant d(d-1) \geqslant 2(n^2+n+1);$$

which holds only for $n \leqslant 1$. This establishes the final contradiction and concludes the proof of the theorem. □

The proof of Theorem 2.1 depends on the irreducibility over $\mathbb{Q}[i]$ of the set of singular points of the Pfaff equation. An irreducibility argument also plays a key rôle in the extension of Jouanolou's result to all smooth projective varieties obtained in [3]. However, in that paper, it is the *universal singular set* that turns out to be irreducible; namely, the set of pairs whose first coordinate is a Pfaff equation ω, and whose second coordinate is a singularity of ω; see [3, Proposition 2.4, p. 122].

3. Reduction modulo p

The constructive proof of Theorem 1.1 that we give in section 4 consists in writing, for any given open set U of $\mathcal{P}_n$, an explicit Pfaff form without algebraic solution that is contained in U. In order to prove that this Pfaff equation does not have algebraic solutions we use Theorem 2.1. This leaves the problem of how one checks the hypotheses of Theorem 2.1 for a Pfaff form that, no matter how carefully constructed, must be quite generic. To get around this problem we use reduction modulo p, as explained in this section.

We begin with a property of prime numbers. Let $n \geqslant 1$ be an integer. We say that a prime p is n-good if

(1) $p \equiv 3 \pmod 4$, and
(2) every prime divisor of $n^2 + n + 1$ divides $p^2 - 1$.

LEMMA 3.1. — *There are infinitely many n-good primes for every $n \geqslant 2$.*

Proof. — Let Q be the square-free factorization of n^2+n+1, and consider the arithmetic progression

$$P_k = (2Q + 1) + 4Qk, \text{ where } k \text{ is a positive integer.}$$

Since $\gcd(2Q + 1, 4Q) = 1$, it follows from Dirichlet's Theorem on primes in arithmetic progressions that there are infinitely many primes of the form P_k. Moreover, $P_k \equiv 3 \pmod 4$; while

$$P_k^2 - 1 = (P_k - 1)(P_k + 1) = 4Q(2k + 1)(Q(2k + 1) + 1),$$

is divisible by Q. Therefore, each prime of the form P_k is n-good. □

Recall that $p \equiv 3 \pmod 4$ if and only if $x^2 + 1$ is irreducible modulo p. Hence,

$$\mathbb{Z}_p[i] = \mathbb{Z}_p[x]/(x^2 + 1),$$

is a field for such a p. If $a \in \mathbb{Z}[i]$, its image in $\mathbb{Z}_p[i]$ will be denoted by $\overline{a}$.

Before we prove the main theorem of this section we need a technical lemma concerning resultants.

LEMMA 3.2. — *Let $n \geqslant 2$ be an integer and let a_0 and b_0 be polynomials of degree at most n in $\mathbb{Z}[i][x, y]$. If $h \in \mathbb{Z}[i][x, y]$ is homogeneous of degree n, and $h(0, y) \neq 0$, then*

$$\deg(\mathrm{Res}_y(hy + a_0, -xh + b_0)) \leqslant n^2 + n + 1.$$

Proof. — To simplify the notation, let

$$a = hy + a_0 \quad \text{and} \quad b = -xh + b_0.$$

Since $xa + yb = xa_0 + yb_0$, it follows that

$$\mathrm{Res}_y(xa, b) = \mathrm{Res}_y(xa_0 + yb_0, b),$$

by [5, Exercise 7, p. 76]. But by [5, Exercise 3, p. 73],

$$\mathrm{Res}_y(xa, b) = \mathrm{Res}_y(x, b)\mathrm{Res}_y(a, b) = x^n \mathrm{Res}_y(a, b),$$

because b has degree n with respect to y. Thus,

$$n + \deg(\mathrm{Res}_y(a, b)) = \deg(\mathrm{Res}_y(xb_0 + ya_0, b)) \leqslant (n+1)^2,$$

since both $xa_0 + yb_0$ and b have total degree at most $n+1$. Therefore,

$$\deg(\mathrm{Res}_y(a, b)) \leqslant (n+1)^2 - n = n^2 + n + 1,$$

as required. □

THEOREM 3.3. — *Let $n \geqslant 2$ be an integer, p an n-good prime, and $\zeta \in \mathbb{Z}[i]$ a number whose residue modulo p generates the group of nonzero elements of $\mathbb{Z}_p[i]$. Suppose that a_0 and b_0 are polynomials of degree at most n in $\mathbb{Z}[i][x, y]$, and that $h \in \mathbb{Z}[i][x, y]$ is homogeneous of degree n with $h(0, y) \neq 0$. If*

(1) $h \equiv x^n \pmod{p}$;
(2) $b_0 \equiv y^n \pmod{p}$; *and*
(3) $a_0 \equiv -\zeta \pmod{p}$;

then the Pfaff form of $\mathbb{P}^2$ induced by $\omega = (hy + a_0)dx + (-xh + b_0)dy$ does not have an algebraic solution.

Proof. — As we did in the previous proof, let

$$a = hy + a_0 \quad \text{and} \quad b = -xh + b_0,$$

and write

$$I = (a, b) \cap \mathbb{Q}[x].$$

By the definition of resultant, the polynomial $R = \mathrm{Res}_y(b, a)$ belongs to I. Now, if

$$R \text{ is irreducible of degree } n^2 + n + 1, \tag{3.1}$$

then, by Theorem 2.1, the Pfaff form of $\mathbb{P}^2$ induced by $adx + bdy$ does not have any algebraic solutions, as required. Therefore, we need only prove that the resultant R satisfies (3.1). This is where we use reduction modulo p.

We begin by computing the reduction $\overline{R}$ of R modulo p. Reducing modulo p the Sylvester matrix that corresponds to (b, a), we obtain

$$S = \begin{bmatrix} -1 & 0 & \cdots & x^{n+1} & \cdots & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 0 & \cdots & x^{n+1} & 0 & \cdots & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & 0 & \cdots & 0 & 0 & 0 & x^{n+1} \\ 0 & 0 & \cdots & x^n & -\overline{\zeta} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & x^n & -\overline{\zeta} & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & x^n & -\overline{\zeta} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & x^n & -\overline{\zeta} \end{bmatrix}.$$

Thus,

$$\overline{R} = \overline{\operatorname{Res}_y(b, a)} = \det(S) = (-1)^{n+1}(x^{n^2+n+1} - \overline{\zeta}^n),$$

which is a polynomial of degree $n^2 + n + 1$ in $\mathbb{Z}_p[i][x]$. Moreover, by [9, Theorem 16, p. 221], the polynomial $x^{n^2+n+1} - \overline{\zeta}^n$ is irreducible in $\mathbb{Z}_p[i]$ as long as $\overline{\zeta}^n$ is not a q-th root in $\mathbb{Z}_p[i]$ for any prime factor q of $n^2 + n + 1$. We prove this last fact.

Assume, by contradiction, that there exists $\beta \in \mathbb{Z}_p[i]$ such that $\overline{\zeta}^n = \beta^q$, with q a prime factor of $n^2 + n + 1$. Then,

$$(\overline{\zeta}^n)^{(p^2-1)/q} = (\beta^q)^{(p^2-1)/q} = 1.$$

Since $\overline{\zeta}$ generates $\mathbb{Z}_p[i]$ by hypothesis, it follows that q must divide n, which is impossible because $\gcd(n, n^2 + n + 1) = 1$. Therefore, $\overline{R}$ is irreducible over $\mathbb{Z}_p[i]$ of degree $n^2 + n + 1$.

In particular, we have that

$$\deg(R) \geqslant \deg(\overline{R}) = n^2 + n + 1.$$

However, by Lemma 3.2, the opposite inequality also holds. Hence,

$$\deg(R) = \deg(\overline{R}) = n^2 + n + 1.$$

Since $\overline{R}$ is also irreducible, we conclude that R itself is irreducible. This shows (3.1) and completes the proof of the theorem. □

4. Proof of Theorem 1.1

Given a set V of $\mathcal{P}_n$, open with respect to the analytic topology, we can choose an element in V of the form α/g, with

$$\alpha = (hy + a_0)dx + (-hx + b_0)dy,$$

where a_0 and b_0 are polynomials of degree less than or equal to n in $\mathbb{Z}[i][x,y]$, $0 \neq h \in \mathbb{Z}[i][x,y]$ is homogeneous of degree n, $h(0,y) \neq 0$, and g is a nonzero integer.

By Lemma 3.1, there are infinitely many n-good primes. Let p be one of them and choose $\zeta \in \mathbb{Z}[i]$ such that $\overline{\zeta}$ generates the group of units of $\mathbb{Z}_p[i]$. Define,

$$\widehat{h} = x^n + pkh$$
$$\widehat{a_0} = -\zeta + pka_0$$
$$\widehat{b_0} = y^n + pkb_0,$$

and

$$\widehat{\alpha}_k = (\widehat{h}y + \widehat{a_0})dx + (-x\widehat{h} + \widehat{b_0})dy.$$

By Theorem 3.3, $\widehat{\alpha}_k$ does not have any algebraic solutions. On the other hand,

$$\frac{\alpha}{g} - \left(\frac{\widehat{\alpha}_k}{1+pgk}\right) = \frac{\eta}{1+pgk} \tag{4.1}$$

where

$$\eta = (y(h - gx^n) + a_0 + g\zeta)dx + (-x(h - gx^n) + b_0 - gy^n)dy.$$

Since η does not depend on k, it follows from (4.1) that

$$\frac{\widehat{\alpha}_k}{1+pk} \to \frac{\alpha}{g} \quad \text{when} \quad k \to \infty.$$

Therefore, $\widehat{\alpha}_k/(1+pgk) \in V$, for $k \gg 0$; which completes the proof of the theorem.

5. An algorithm

Recall from section 2 that the space $\mathcal{P}_n$ of Pfaff forms of degree $n \geqslant 2$ can be identified with the set of nonzero triples (h, a_0, b_0), where h is a homogeneous polynomial of degree n and a_0, b_0 have degree at most n. Thus

$$\mathcal{P}_n \cup \{0\} \cong \mathbb{R}^{(n+2)(2n+3)}$$

under the identification given above. In particular, the norm $\|\cdot\|_\infty$ is defined in $\mathcal{P}_n$, and every Zariski subset of $\mathcal{P}_n$ is closed under the topology defined by this norm.

We finish with an algorithm, based on the proof of Theorem 1.1 given in the previous section, that explicitly computes a 1-form without algebraic solutions in a neighbourhood of any given 1-form with coefficients in $\mathbb{Q}[i]$.

ALGORITHM 5.1. — *Given an integer $L \geqslant 2$ and a 1-form $\alpha = \alpha/g$, where $\alpha = (hx + a_0)dx + (-hy + b_0)dy$ has coefficients in $\mathbb{Z}[i]$, $g \in \mathbb{Z}$, and $h(0, y) \neq 0$, the algorithm computes a 1-form $\widehat{\alpha}$ and a nonzero integer β, such that:*

- $\|\alpha - \widehat{\alpha}/\beta\|_\infty < 1/L$ *and*
- *the Pfaff form of $\mathbb{P}^2$ obtained by homogenizing $\widehat{\alpha}$ does not have any algebraic solutions.*

Step 1: *Let $n = \deg(\alpha)$.*

Step 2: *Factor $n^2 + n + 1$ and let Q be the product of its prime factors taken with multiplicity one.*

Step 3: *Choose a prime p in the arithmetic progression $(2Q+1)+4Qk$, where $k \geqslant 1$ is an integer.*

Step 4: *Choose $\zeta \in \mathbb{Z}[i]$, such that $\overline{\zeta}$ is a primitive root of unity in $\mathbb{Z}_p[i]$, and an integer*

$$m > \frac{L}{g^2 p} \sup \{\|h - gy^n\|_\infty, \|a_0 - g\zeta\|_\infty, \|b_0 - gy^n\|_\infty\}$$

Step 5: *Set*

$$\begin{aligned} \widehat{h} &= x^n + mph, \\ \widehat{a}_0 &= -\zeta + mpa_0, \\ \widehat{b}_0 &= y^n + mpb_0, \end{aligned}$$

and return

$$\frac{(\widehat{h}y + \widehat{a}_0)dx + (-x\widehat{h} + \widehat{b}_0)dy}{1 + mpg}.$$

This algorithm has been implemented in the computer algebra system AXIOM, see [6]. Experiments have shown that the required primes in the arithmetic progression at Step 3 occur at such large numbers, that it is better to run a simple-minded search for an adequate p among all the primes of the form $4n + 3$. AXIOM is available for download from

`http://page.axiom-developer.org/zope/Plone`;

while the implementation of the algorithm can be found at

`htt://www.dcc.ufrj.br/~collier/folia.html`.

BIBLIOGRAPHY

[1] M. Brunella, "Some remarks on indices of holomorphic vector fields", *Publ. Mat.* **41** (1997), no. 2, p. 527-544.

[2] D. Cerveau & A. L. Neto, "Holomorphic foliations in $\mathbf{CP}(2)$ having an invariant algebraic curve", *Ann. Sc. de l'Institute Fourier* **41** (1991), p. 883-903.

[3] S. C. Coutinho & J. V. Pereira, "On the density of algebraic foliations without algebraic invariant sets", *J. Reine Angew. Math.* **594** (2006), p. 117-135.

[4] S. C. Coutinho & L. M. Schechter, "Algebraic solutions of Holomorphic Foliations: an Algorithmic Approach", *Journal of Symbolic Computation* **41** (2006), p. 603-618.

[5] D. Cox, J. Little & D. O'Shea, *Using algebraic geometry*, Undergraduate Texts in Mathematics, Springer, New York, 1998.

[6] T. Daly, *Axiom: the thirty year horizon, volume 1: tutorial*, Lulu Press, 2005.

[7] G. Darboux, "Mémoire sur les équations différentielles algébriques du I^{o} ordre et du premier degré", *Bull. des Sc. Math. (Mélanges)* (1878), p. 60-96, 123-144, 151-200.

[8] J. P. Jouanolou, *Equations de Pfaff algébriques*, Lect. Notes in Math., vol. 708, Springer-Verlag, Heidelberg, 1979.

[9] S. Lang, *Algebra*, Addison-Wesley, Reading, 1974.

[10] A. J. Maciejewski, J. M. Ollagnier, A. Nowicki & J. M. Strelcyn, "Around Jouanolou non-integrability theorem", *Indag. Mathem.* **11** (2000), p. 239-254.

[11] A. L. Neto, "Algebraic solutions of polynomial differential equations and foliations in dimension two", in *Holomorphic Dynamics* (New York-Heidelberg-Berlin), Lect. Notes in Math., vol. 1345, 1988, p. 192-232.

[12] J. M. Ollagnier, A. Nowicki & J. M. Strelcyn, "On the non-existence of constants of derivations: the proof of a theorem of Jouanolou and its development", *Bull. Sci. math.* **123** (1995), p. 195-233.

[13] M. J. Prelle & M. F. Singer, "Elementary first integrals of differential equations", *Trans. Amer. Math. Soc.* **279** (1983), no. 1, p. 215-229.

Manuscrit reçu le 16 mai 2006,
accepté le 22 août 2006.

S. C. COUTINHO
Universidade Federal do Rio de Janeiro
Departamento de Ciência da Computação
Instituto de Matemática
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)
collier@impa.br