Algorithms For Recognizing Coordinates In Two Variables Over UFD’s

Hassan El Houari
Department of Mathematics
Faculty of Sciences Semlalia
University Cadi Ayyad
P. O. Box 2390, Marrakech, Morocco
h.elhouari@ucam.ac.ma

M’hammed El Kahoui
Department of Mathematics
Faculty of Sciences Semlalia
University Cadi Ayyad
P. O. Box 2390, Marrakech, Morocco
elkahoui@ucam.ac.ma

ABSTRACT
We give an easy and efficient algorithm to check whether a given polynomial \( f \) in \( K[x, y] \) is a coordinate, where \( K \) be a commutative field of characteristic zero, and if so to compute a coordinate’s mate of \( f \). Then we treat the same problem replacing the ground field \( K \) by a unique factorization domain \( A \) of characteristic zero. A notable feature of our method is that it always produces a mate of minimum degree.

Categories and Subject Descriptors
I.1.2 [Symbolic and Algebraic Manipulation]: Algorithms—Algebraic algorithms; F.2.1 [Analysis of Algorithms and Problem Complexity]: Numerical Algorithms and Problems—Computations on polynomials

General Terms
Algorithms

Keywords
Coordinate, Locally nilpotent derivation, Slice

1. INTRODUCTION
Let \( K \) be a commutative field of characteristic zero and \( K[x_1, \ldots, x_n] = K[x] \) be the ring of polynomials in \( n \) indeterminates with coefficients in \( K \). A polynomial \( f \) in \( K[x] \) is called a coordinate if there exist polynomials \( f_1, \ldots, f_{n-1} \) such that \( K[x] = K[f, f_1, \ldots, f_{n-1}] \). Deciding whether a given polynomial \( f \) is a coordinate is one of the most fundamental problems in the study of automorphisms of polynomial rings.

To our knowledge this problem is still open for \( n \geq 3 \). In the case of two variables it is solved by the famous Abhyankar-Moh theorem [1] which states that \( f \) is a coordinate if and only if \( I(\partial_x f, \partial_y f) = \{1\} \) and the curve \( C(f) \) defined by \( f = 0 \) has one place at infinity. Since then, various and more or less explicit solutions have been given to this problem, see e.g. [4, 8, 5, 11, 3]. However, the closely related question of computing a coordinate’s mate, i.e. a polynomial \( g \) such that \( K[f, g] = K[x, y] \), is either not treated or solved in a more or less involved way, see [2]. For instance, in [5] an integral formula is given for computing a Jacobian mate, i.e. a polynomial \( g \) such that \( \text{Jac}(f, g) = 1 \), and as by-product it solves the question of coordinate’s mate. In [11] the same question is solved by keeping track of the so-called nonsingular Gröbner reductions performed to check whether \( f \) is a coordinate.

In this work we build on the results of van den Essen [8], so let us recall some of them. Given a polynomial \( f \in K[x, y] \) we let \( X_f = \partial_y f \partial_x - \partial_x f \partial_y \) be the Hamiltonian \( K \)-derivation associated to it. The main result of concern for our purpose states that \( f \) is a coordinate if and only if \( X_f \) is locally nilpotent and \( I(\partial_x f, \partial_y f) = \{1\} \). Moreover, deciding whether \( X_f \) is locally nilpotent reduces to check whether \( X_f^{d+1}(x) = X_f^{d+1}(y) = 0 \), where \( d \) is the total degree of \( f \). Thus, deciding whether \( f \) is a coordinate reduces to explicit and well controlled algebraic computations. On the other hand, the question of computing a coordinate’s mate for \( f \) is reduced to compute a slice of \( X_f \), i.e. an element \( s \) such that \( X_f(s) = 0 \).

In this paper we show that the necessary computations performed to check whether \( X_f \) is locally nilpotent, namely the computation of the iterates \( X_f^i(x) \) and \( X_f^i(y) \) up to the bound \( \text{deg}(f) + 1 \), are enough for checking whether \( f \) is a coordinate and for computing a coordinate’s mate in case it exists. We then extend the obtained result over fields to UFD’s of characteristic zero, and as by-product we give an algorithm which allows to recognize coordinates in two variables over such rings.

The paper is structured as follows: in section 2 we give some basic results concerning locally nilpotent derivations and coordinates in two variables. Section 3 is devoted to the problem of algorithmically recognizing coordinates and computing mates over fields of characteristic zero. In section 4 we show that the method we describe always produces a younger mate. In section 5 we study coordinates in two variables over UFD’s of characteristic zero. We give algorithmic solutions to both the recognition and the mate problems. In section 6 we give some details on implementations and we study some examples.

2. BASIC FACTS
Let \( A \) be a commutative ring with unit containing the rational numbers, \( A[t] \) is a univariate polynomial ring and \( X \) be a locally nilpotent derivation on \( A \). For any \( a \in A \) the exponential \( \exp(tX).a \) is usually defined as

\[
\exp(tX).a = \sum_i \frac{X^i(a)}{i!} t^i.
\]

The degree of \( a \) with respect to \( X \) is defined as \( \deg_X a = \deg_2(\exp(tX).a) \).

Let us recall some classical results that we will use in the sequel. The first one concerns automorphisms of the affine plane and it can be found in [10].

**Lemma 2.1.** Let \( A \) be a domain of characteristic zero and \((f, g)\) be an automorphism of \( A[x, y] \), and let \( \deg(f(0, y)) = d_1 \) and \( \deg(g(0, y)) = d_2 \). Then \( \deg_2(f) = d_1 \) and \( \deg_2(g) = d_2 \), and if moreover both \( d_1 \) and \( d_2 \) are positive then the leading coefficients of \( f \) and \( g \) with respect to \( y \) are constants and \( d_1|d_2 \) or \( d_2|d_1 \).

The second one is a particular case of proposition 1.1.31 in [6].

**Lemma 2.2.** Let \( K \) be a commutative field and let \( f, g \) be two polynomials in \( K[x, y] \) such that \( J_{x}(f, g) = 1 \), then \( f \) and \( g \) are algebraically independent over \( K \).

A basic fact on slices of locally nilpotent derivations is given in the following theorem which can be found in [9, 12]. The proof we supply here is elementary and constructive.

**Theorem 2.3.** Let \( A \) be a UFD of characteristic zero and \( X = X_1 \) be a locally nilpotent derivation of \( A[x, y] \), and assume that \( X \) has a slice \( y \). Then \( A[x, y]^{X_1} = A[f] \) and \( A[x, y] = A[f, g] \).

**Proof.** The case where \( f \) is linear being trivial, we will assume in the sequel that \( f \) is nonlinear. Let \( P \) be a polynomial in \( A[x, y]^{X_1} \), by induction on the degree of \( P \) we will prove that \( P \in A[f] \). The case when \( \deg(P) = 0 \) is clear. Assume now that the result remains true for every polynomial of degree at most \( m \) and let \( P \) be a polynomial of \( A[x, y]^X \) of degree \( m + 1 \). We have then

\[
\partial_y f \partial_x P - \partial_x f \partial_y P = 0.
\]

On the other hand we have

\[
\partial_y f \partial_x g - \partial_x f \partial_y g = 1.
\]

From the two last equalities we obtain the relations

\[
\begin{align*}
\partial_x P &= F(x, y) \partial_x f, \\
\partial_y P &= F(x, y) \partial_y f,
\end{align*}
\]

where \( F(x, y) = \partial_x g \partial_y P - \partial_y g \partial_x P \). Since \( f \) is nonlinear we have \( \deg(F) \leq m \). On the other hand, an easy computation shows that \( \partial_x F \partial_y f - \partial_y F \partial_x f = 0 \). By induction hypothesis we may write \( F(x, y) = h(f) \) with \( h \in A[t] \). This proves that \( P = H(f) \) where \( H \in K[t] \) is such that \( H' = h \) and \( K \) is the quotient field of \( A \).

Now we turn to prove that \( H \) has its coefficients in \( A \). Since \( A \) is a UFD we may find an element \( \beta \) of \( A \) such that \( H_1 = \beta H \in A[t] \) and \( H_1(t) \) is primitive. We therefore have \( \beta P(x, y) = H_1(f) \), which gives

\[
H_1(f) = 0 \mod \beta.
\]

Assume that \( \beta \) is not a unit in \( A \) and let \( c \) be a prime factor of \( \beta \). On the first hand, the fact that \( \chi_f(g) = 1 \) implies that \( f \) is nonconstant in \((A/c)[t] \). On the other hand, equation (2.1) gives

\[
H_1(f) = 0 \mod c,
\]

and hence \( H_1(f) = 0 \mod c \) according to the fact that \( A/c \) is a domain and \( f \) is nonconstant in \((A/c)[t] \). But this means that \( c \) divides the coefficients of \( H_1 \), and contradicts the fact that \( H_1 \) is primitive. Thus, \( \beta \) is a unit in \( A \) and so \( H \) has its coefficients in \( A \).

The fact that \( X \) remains locally nilpotent in \( K[x, y] \) implies that \((f, g)\) is an automorphism of \( K[x, y] \). Let \((f_1, g_1)\) be the inverse of \((f, g)\), and let us prove that \( f_1 \) and \( g_1 \) are in fact polynomials in \( A[x, y] \). Since \( A \) is a UFD we may find an element \( \lambda \) of \( A \) such that \( f_2 = \lambda f_1 \) is primitive in \( A[x, y] \).

Assume that \( \lambda \) is not a unit of \( A \) and let \( c \) be a prime divisor of \( \lambda \). From the identity \( f_2(f, g) = \lambda x \) we deduce that

\[
f_2(f, g) = 0 \mod (c),
\]

and by lemma 2.2 we get

\[
f_2(x, y) = 0 \mod (c).
\]

But this means that \( c \) divides all the coefficients of \( f_2 \), and this contradicts the assumption that \( f_2 \) is primitive. Thus \( \lambda \) is a unit in \( A \) and so \( f_1 \) has its coefficients in \( A \). In the same way we prove that \( g_1 \in A[x, y] \).

**3. Recognizing Coordinates and Computing Mates in the Case of a Field**

A polynomial \( f \in K[x, y] \) is called triangular if it is of the type \( ay + p(x) \) or \( bx + q(y) \). Notice that a triangular polynomial \( f = ay + p(x) \) is a coordinate if and only if \( a \in K^* \), and if so \( g = x \) is a coordinate’s mate of \( f \). The triangular case being trivial, we will assume in this case that the considered polynomials are non-triangular. We have now enough material to state the main result of this section.

**Theorem 3.1.** Let \( K \) be a commutative field of characteristic zero and \( f \) be a non-triangular polynomial in \( K[x, y] \). Then \( f \) is a coordinate if and only if the following two conditions hold:

i) the derivation \( X_1 \) is locally nilpotent,

ii) \( r_1 = \deg_X X_1 \geq 2 \) and \( X_1 r_1(x) \) is constant.

In this case, also \( r_2 = \deg_X y \geq 2 \) and \( X_1 r_2(y) \) is constant and \( X_1 r_2^{-1}(x) \), as well as \( X_1 r_2^{-1}(y) \), is a coordinate’s mate of \( f \).

**Proof.** “ \( \Rightarrow \)” Let \( g \) be a coordinate’s mate of \( f \). Without loss of generality we may assume that \( X_1(g) = 1 \). This proves in particular that \( X_1^2(g) = 0 \). Since on the other hand \( X_1(f) = 0 \) and \( K[x, y] = K[f, g] \) we deduce that \( X_1 \) is locally nilpotent.

Let \((f_1, g_1)\) be the inverse of \((f, g)\). So \( x = f_1(f, g) \). Since \( X_1 = \frac{d}{dy} \) it follows that

\[
X_1(x) = (\partial_y f_1)(f, g)
\]

for all \( i \). Write \( f_1 = \sum a_i(x)y^i \), with \( \deg_y f_1 = r \). Then by lemma 2.1 \( a_r \in K^* \) and hence \( X_1^r(x) = r!a_r \in K^* \). This
shows that $\deg X_t x = r$. The fact that $r \geq 2$ follows from the assumption that $f$ is non divisible.

Finally, $X_t^{-1}(x) = r a_g + (r - 1)! a_{r-1}(f)$, which clearly is a coordinate's mate of $f$.

"⇐" By theorem 2.3 we have $\mathcal{K}[x,y] = \mathcal{K}[f,g]$, where $g = (X_t^{-1}(x))^{-1} X_t^{-1}(x)$.

From the proof of theorem 3.1 we deduce a formula which gives an expression of the inverse of an automorphism of $\mathcal{K}[x,y]$. In fact, this can be established in the more general case of automorphisms of the ring $\mathcal{A}[x_1, \ldots, x_n]$, where $\mathcal{A}$ is a commutative ring with unit containing the rationals. Before giving this, we need to fix some notations. Given $n - 1$ polynomials $f_1, \ldots, f_{n-1}$ in $\mathcal{A}[x] = \mathcal{A}[x_1, \ldots, x_n]$ we let $X_{f_1, \ldots, f_{n-1}}(x)$ be the $\mathcal{A}$-derivation of $\mathcal{A}[x]$ defined by $X_{f_1, \ldots, f_{n-1}}(f) = \text{Jac}(f_1, \ldots, f_{n-1}, f)$, where $\text{Jac}$ stands for the Jacobian determinant operation. When $F = (f_1, \ldots, f_n)$ is an $\mathcal{A}$-automorphism of $\mathcal{A}[x]$, the derivation $X_{f_1, \ldots, f_{n-1}}$ is locally nilpotent since we have $X_{f_1, \ldots, f_{n-1}}(F) = \delta_h$.

**Proposition 3.2.** Let $F = (f_1, \ldots, f_n)$ be an $\mathcal{A}$-automorphism of $\mathcal{A}[x]$ with 1 as Jacobian determinant, and $G = (g_1, \ldots, g_n)$ be its inverse. Then for any $i = 1, \ldots, n$ we have:

$$\exp(t X_{f_1, \ldots, f_{n-1}}), x_i = g_i(f_1, \ldots, f_{n-1}, t + f_n).$$

**Proof.** Applying $X_{f_1, \ldots, f_{n-1}}$ to the equation

$$x_i = g_i(f_1, \ldots, f_n)$$

we get

$$X_{f_1, \ldots, f_{n-1}}(x_i) = (\partial_{x_i} g_i)(f_1, \ldots, f_n),$$

and by induction we easily prove that

$$X_{f_1, \ldots, f_{n-1}}(x_i) = (\partial_{x_i} g_i)(f_1, \ldots, f_n)$$

for any $k$. Taking into account these relations we get

$$\exp(t X_{f_1, \ldots, f_{n-1}}), x_i = \sum_k \frac{1}{k!} (\partial_{x_i} g_i)(f_1, \ldots, f_n)^k.$$  

The right hand side of the last equation is nothing but the Taylor expansion of $g_i(f_1, \ldots, f_{n-1}, t + f_n)$ around $f_n$.

**4. THE QUESTION OF YOUNGER MATE**

In this section we show that the coordinate's mate computed in theorem 3.1 is always a younger mate of the given polynomial.

**Lemma 4.1.** Let $A$ be a domain and let $f, g \in \mathcal{A}[t]$ be two polynomials such that $\deg(f) = p$, $\deg(g) = q$ and $\min(p, q) \geq 2$. Let $\text{Res}(f, t - x, g, y - y)$ be the resultant of $f(t) - x$ and $g(t) - y$ with respect to $t$. Then $\deg_x(\text{Res}(f, t - x, g, y - y)) = q$, $\deg_y(\text{Res}(f, t - x, g, y - y)) = p$ and the leading coefficients of $\text{Res}(f, t - x, g, y - y)$ with respect to both $x$ and $y$ are constants.

**Proof.** Let us write $f = c_0 t^p + \ldots + c_0$ and $g = d_0 t^q + \ldots + d_0$. Let $\text{Sylv}(f(t) - x, g(t) - y) = (a_{i,j})$ be the Sylvester matrix of $f(t) - u$ and $g(t) - v$. The coefficients $a_{i,j}$ are either constants or $c_0 - x$ or $d_0 - y$. Moreover, the number of times $c_0 - x$ (resp. $d_0 - y$) appears in $\text{Sylv}(f(t) - x, g(t) - y)$ is $q$ (resp. $p$). Since on the other hand $\text{Res}(f, t - x, g, y - y)$ is the determinant of the Sylvester matrix, we have the bounds $\deg_x(\text{Res}(f, t - x, g, y - y)) \leq q$, $\deg_y(\text{Res}(f, t - x, g, y - y)) \leq p$.

To prove that these bounds are equalities we need to be little bit more precise, and give the exact subscripts $j, k$ whose corresponding coefficient is $c_0 - x$ (resp. $d_0 - y$).

In fact we have $a_{j,k} = d_0 - y$ and if only if $j + 1 + k > l$. Let us write

$$\text{Res}_k(f - x, g - y) = \sum_{\sigma \in S_{l+p+q}} \varepsilon(\sigma) a_{1, \sigma(1)} \cdot \cdots \cdot a_{p+q, \sigma(p+q)}.$$  

In order that a given $\sigma$ generates a term of the type $c(d_0 - y)^p$ it should satisfy $\sigma(j) = j$ for any $j \geq q + 1$. This means in particular that $\sigma(j) \leq q$ for any $j \leq q$. Therefore, the coefficient of the monomial $(d_0 - y)^p$ in $\text{Res}_k(f - x, g - y)$ is $d_0, q$, where $A_{q,q}$ is the $q \times q$ principal submatrix of $\text{Sylv}(f(t) - x, g(t) - y)$. Clearly, $A_{q,q}$ is upper triangular and its diagonal entries are equal to $c_y$. Thus, we have $\text{Res}_k(f - x, g - y) = \text{Res}_l(d_0 - y)^p + r(x, y)$ with $\deg_y(r) < p$.

Similar arguments show that $\text{Res}_k(f - x, g - y)$ is of degree $q$ with respect to $x$ and its leading coefficient is constant.

**Lemma 4.2.** Let $(f, g)$ be an automorphism of $\mathcal{K}[x,y]$ and assume that $\deg(f) > \deg(g)$. Let $(f_1, g_1)$ be the inverse of $(f, g)$ and write $f_1 = a_1 y^m + a_{m-1}(x) y^{m-1} + \ldots + a_0(x)$ and $g_1 = b_1 y^q + b_{q-1}(x) y^{q-1} + \ldots + b_0(x)$. Then the coefficients $a_{m-1}$ and $b_{q-1}$ are constants.

Even if it means replacing $(f, g)$ by $(f \circ t, g \circ t)$, where $t$ is a suitable linear transformation, we may assume that $\deg_y(f) = \deg(f)$ and $\deg_x(g) = \deg(g)$. Indeed, such change of coordinates does not affect the condition $\deg_y(f) < \deg(f)$. Moreover, since the inverse of $(f \circ t, g \circ t)$ is $t^{-1} \circ (f_1, g_1)$ the claimed conclusion will not be modified.

Let $a, b$ be new indeterminates. Since $(f, g)$ is an automorphism, then by Theorem 3.1.1 in [6] the resultant of $f - u$ and $g - v$ with respect to $y$ writes as

$$\text{Res}_y(f - u, g - v) = a(x - f_1(u, v)).$$

If we let $m = \deg_y(f)$ and $n = \deg_x(g)$, then by lemma 4.1 $f_1(u, v)$ is a polynomial of degree $m$ with respect to $v$ and of degree $n$ with respect to $u$ and its leading coefficients with respect to both $u$ and $v$ are constants. Since the degree of the inverse $(f_1, g_1)$ equals the degree of $(f, g)$ we deduce that $f_1$ is of degree $m$.

Let $h_m$ be the leading homogeneous term of $f_1$. Then $h_m$ is a power of a linear form $ax + bu$ and since $\deg_x(h_m) = \deg_x(f_1) = n < m$ we have $b = 0$. This proves that $a_{m-1}(x)$ is constant. The fact that $b_{q-1}(x)$ is also constant follows immediately from the Jacobian condition.

**Theorem 4.3.** Let $K$ be a commutative field of characteristic zero and $f$ be a non-trivial coordinate in $\mathcal{K}[x,y]$. Then $X_{f}(x) = \mathcal{K}[x]$, as well as $(X^{q-1}_f(y))^{-(q-1)x}}^{\mathcal{K}[x]}$ is a younger mate of $f$.

**Proof.** Let $g$ be a younger mate of $f$ such that $Jac(f, g) = 1$ and let $(f_1, g_1)$ be the inverse of $(f, g)$. Let us write

$f_1 = a_p y^p + a_{p-1}(x) y^{p-1} + \ldots + a_0(x)$

$g_1 = b_q y^q + b_{q-1}(x) y^{q-1} + \ldots + b_0(x)$

By lemma 4.2 the coefficients $a_{m-1}(x)$ and $b_{q-1}(x)$ are constant, and taking into account the algebraic identities in proposition 3.2.3 we obtain the equations

$X^{q-1}_f(x) = p a_0 a_1 \ldots a_p$, $X^{q-1}_f(x) = (p - 1)! (a_{p+q-1})$, $X_f(y) = q b_0 q_1 \ldots b_q$.
Therefore \((X_f^j(x))^{-1}A_f^{j-1}(x) = g + (pa_p)^{-1}a_{p-1}\), and this proves the claimed result. 

5. THE CASE OF A UFD OF CHARACTERISTIC ZERO

In this section we address the same problem replacing the ground field \(K\) by a unique factorization domain of characteristic zero \(A\).

**Theorem 5.1.** Let \(A\) be a UFD of characteristic zero and \(f\) be a polynomial in \(A[x, y]\). Then \(f\) is a coordinate if and only if the following conditions hold:

i) the derivation \(X_f\) is locally nilpotent,

ii) \(X_f(x)\) is constant.

In this case, \((X_f^j(x))^{-1}(X_f^{j-1}(x) - h(f))\) is a coordinate’s mate of \(f\).

**Proof.** “\(\Rightarrow\)” The conditions i) and ii) can be checked in the same way as in the proof of theorem 3.1, so the only one thing that remains is to prove the condition iii). Let \(g\) be a coordinate’s mate of \(f\) such that \(X_f(g) = 1\). Then

\[X_f(A_f^{j-1}(x) - X_f^{j-1}(x)g) = 0,\]

and so \(X_f^{j-1}(x) - X_f^{j-1}(x)g = h(f)\) according to theorem 2.3.

“\(\Leftarrow\)” By theorem 2.3 it is enough to prove that \(X_f\) has a slice. Since we have \(X_f^{j-1}(x) = h(f)\) mod \(X_f^j(x)\)\), there exists a polynomial \(g\) in \(A[x, y]\) such that \(X_f^{j-1}(x) = h(f) + (X_f^j(x))g\), which implies that \(X_f(g) = 1\).

In order to translate the last theorem into an algorithm we need to give an efficient solution to the following problem.

**Problem:**

Let \(A\) be a UFD and \(a\) be a nonzero element of \(A\). Let \(f, g \in A[x, y]\). How to check whether \(g = h(f)\) mod \(a\), where \(h\) is a polynomial in \(A[t]\)?

In the sequel, \(\text{Rem}(g, f; y)\) will stand for the Euclidean remainder of \(g\) by \(f\) with respect to the variable \(y\), which is an element of \(K[x, y]\) where \(K\) be the quotient field of \(A\). The following lemma is the master piece of the solution we give to this problem.

**Lemma 5.2.** Let \(A\) be a domain and \(f, g \in A[x, y]\). Then \(g = h(f)\) if and only if \(\text{Rem}(g, f - t; y) = h(t)\), where \(h\) is a polynomial in \(A[t]\).

**Proof.** “\(\Leftarrow\)” Assume that \(\text{Rem}(g, f - t; y) = h(t)\) then \(g = h(t)\) mod \((f - t)\) and by substituting \(f\) to \(t\) we get \(g = h(f)\).

“\(\Rightarrow\)” If \(g = h(f)\) then \(g - h(t) = h(f) - h(t) = (f - t)P\) where \(P\) a polynomial in \(A[x, y, t]\), and since \(\deg(h) < \deg(f)\) then \(\text{Rem}(g, f - t; y) = h(t)\).

Let \(A\) be a UFD, \(f, g\) be polynomials in \(A[x, y]\) and \(a\) be an element of \(A\). We may write \(a = a_1\cdots a^m\), where the \(a_i\)’s are irreducible. By using Euclidean division over the domain \(A/(a_1)\) we let

\[h_{i,1}(t) = \text{Rem}(g, f - t; y) \mod (a_i),\]

and then for \(j = 2, \ldots, m_1\) we let

\[h_{i,j}(t) = \text{Rem}(g_{i,j-1}, f - t; y) \mod (a_i),\]

\[g_{i,j} = a_i^{-1}(g - h_{i,j}(f)).\]

We repeat the same process for \(a_2, a_3, \ldots, a_r\) by letting for any \(i = 2, \ldots, r\)

\[h_{i,j}(t) = \text{Rem}(g_{i-1,m_i-1}, f - t; y) \mod (a_i),\]

\[g_{i,j} = a_i^{-1}(g - h_{i,j}(f)).\]

where \(j = 1, \ldots, m_i\) and \(g_{i,0} = g_{i-1,m_i-1}\). The solution of our problem is stated in the following theorem.

**Theorem 5.3.** Let \(A\) be a UFD, \(f, g\) be two polynomials in \(A[x, y]\) and \(a\) be a nonzero element of \(A\). Let us write \(a = a_1a_2\cdots a_m\), where the \(a_i\)’s are prime in \(A\). Then the following assertions are equivalent:

i) \(g = h(f)\) mod \(a\) for some \(h \in A[t]\),

ii) all the \(a_i\)’s are elements of \(A[t]\).

In this case the polynomial \(h = \sum_{i=1}^m a_i^{-1}h_{i,j}(t)\) satisfies \(g = h(f) + ag_{r,m}\).

**Proof.** “\(i \Rightarrow ii\)” This is a direct consequence of the routine described above and lemma 5.2.

“\(ii \Rightarrow i\)” We will prove this by induction on the “size” \(m = m_1 + \cdots + m_r\) of \(a\). The case \(m = 1\) being trivial, assume that the result holds for elements of size \(\leq m\) and let \(a\) be with size \(m + 1\). Let \(a_1\) be a prime factor of \(a\). By using Euclidean division over the domain \(A/(a_1)[x, t]\) we have \(g = h_{1,1}(f) + a_1g_{1,1}\), and applying the induction hypothesis to \(g_{1,1}\) and \(a_1^{-1}\), we get \(g_{1,1} = h'(f) \mod (a_1^{-1}a)\) for some \(h' \in A[t]\). Therefore, \(g = h(f) \mod (a)\), where \(h(t) = h_{1,1}(t) + a_1h'(t)\).

6. IMPLEMENTATION

In this section we give a pseudo-code description of the algorithm studied in the previous sections. The algorithm takes as input a polynomial \(f\) in two variables with coefficients in a UFD of characteristic zero and checks whether it is a coordinate, and if so it computes a coordinate’s mate. Moreover it produces a mate of \(f\) of minimum degree.

6.1 Description of the algorithm Coordinate

For a given polynomial \(f\) the algorithm performs the following steps:

**step 1:** It is well known that the leading homogeneous form of \(f\) should be a power of a linear form. Thus in this step we test if \(f\) satisfies this condition.

**step 2:** We test by using an algorithm called LN if the \(K\)-derivation \(X_f\) is locally nilpotent, by computing the iterates \(X_f^j(x)\) and \(X_f^j(y)\) up to \(d = \deg(f)\). At the same time we check whether \(X_f^{j-1}(x)\) is constant, where \(r_1 = \deg X_f(x)\). Notice that according to the relation (3.1) the degree of the \(i\)-th iterate should be bounded by \(\min(d - 1, i(d - 2) + 1)\). The computation is stopped if the degree of \(X_f^{j-1}(x)\) exceeds this bound. If \(X_f^{j-1}(x)\) divides \(X_f^{j-1}(x)\), the polynomial \((X_f^{j-1}(x))^{-1}X_f^{j-1}(x)\) is a younger mate of \(f\). Otherwise, the algorithm returns the polynomial \((X_f^{j-1}(x))^{-1}X_f^{j-1}(x)\) and the constant \(X_f^{j-1}(x)\).
step 4: In case a mate is computed in the step 4, we transform it into a mate of minimum degree by using an algorithm called RED.

The Algorithm Coordinate

Input: A polynomial \( f \in \mathcal{A}[x,y] \), where \( \mathcal{A} \) is a UFD.
output: Either a message that \( f \) is not coordinate or a mate with minimum degree \( g \in \mathcal{A}[x,y] \) of \( f \).

Begin
If \( \text{deg}_y(\text{coeff}(f,y)) \neq 0 \) Then
Return \( (f \text{ is not coordinate}) \);
EndIf;
\( F := \text{homogeneous}(f,x,y,t) \);
\( f_n := F(x,y,0) \);
\( d_1 := \partial_x f_n ; d_2 := \partial_y f_n \);
\( k_1 := \text{gcd}(f_n,d_1) ; k_2 := \text{gcd}(f_n,d_2) \);
If \( d_1 \neq 0 \) and \( \text{deg}_y(k_1) \neq \text{deg}_y(d_1) \) Then
Return \( (f \text{ is not coordinate}) \);
Else If \( d_2 \neq 0 \) and \( \text{deg}_y(k_2) \neq \text{deg}_y(d_2) \) Then
Return \( (f \text{ is not coordinate}) \);
EndIf;
\( N := \text{LN}(f) \);
If \( \text{nops}(N) = 0 \) Then Return \( (f \text{ is not coordinate}) \);
EndIf;
If \( \text{Divide}(N[1],N[2],\text{'q'}) \) Then
If \( \text{content}(q) \) is integer Then
Return \( (q) \);
EndIf;
EndIf;
\( H := \text{SEQ}(F,N[1],N[2]) \);
If \( \text{nops}(H) = 0 \) Then Return \( (f \text{ is not coordinate}) \);
EndIf;
If \( \text{content}(H[1]) \) is integer Then
Q := \text{RED}(f,H[1],X,Y) ;
Return \( (Q[1]) \);
Else Return \( (f \text{ is not coordinate}) \);
EndIf;
End;
End;

The Algorithm SEQ

Input: Two polynomials \( f, g \in \mathcal{A}[x,y] \) and an element \( a \in \mathcal{A} \).
output: \( h \in \mathcal{A}[t] \) and \( \bar{g} \in \mathcal{A}[x,y] \) such that \( g = h(f) + a \bar{g} \), in case a decomposition exists.

Begin
If \( \text{factor}(d) \) Then
\( G_{1,0} := g ; F := f; \)
For \( i \) from 1 to \( \text{nops}(r[2]) \) Do
\( \text{mod}_i := \text{MOD}(F,r[2][i][1]) ; \)
For \( j \) from 1 to \( r[2][i][2] \) Do
\( \text{mod}_i := \text{MOD}(G_{i,j-1},r[2][i][1]) ; \)
\( h_{i,j} := \text{Rem}(\text{mod}_i,\text{mod}_f - t,y) ; \)
\( G_{i,j} := (G_{i,j-1} - \text{subs}(t=F,h_{i,j}))/r[2][i][1] ; \)
If \( G_{i,j} \) is polynomial Then
If \( h_{i,j} <> 0 \) and \( \text{degree}(h_{i,j},x,y) <> 0 \) Then
Return \( ([]) \);
Else \( H := H + r[2][i][1]^{j-1}h_{i,j} ; \)
EndIf;
Else \( G_{i,j} := G_{i,j-1} ; \)
EndIf;
EndDo;
EndIf;
\( G_{i+1,0} := G_{i,r[2][i][2]} ; F := \text{mod}_f ; \)
EndDo;
Return \( ([G_{\text{nops}(r[2]),r[2][\text{nops}(r[2])][2]/r[1][1],H]) ; \)
End;

The Algorithm MOD

Input: A polynomial \( f \) and an element \( d \in \mathcal{A} \).
output: The residue-class \( f \) of \( f \) modulo \( d \).

Begin
\( f_1 := f ; F := 0 ; \)
While \( f_1 <> 0 \) Do
\( \text{coeff} := \text{leadcoeff}(f_1,t\text{deg}(X,Y)) ; \)
If \( \text{divide}(\text{coeff},d) \) Then
Else
\( F := F + \text{coeff} * \text{leadterm}(f_1,t\text{deg}(X,Y)) ; \)
EndIf;
\( f_1 := f_1 - \text{coeff} * \text{leadterm}(f_1,t\text{deg}(X,Y)) ; \)
EndDo;
Return \( (F) \);
End;

The Algorithm LN

Input: \( f \in \mathcal{A}[x,y] \) where \( \mathcal{A} \) is a UFD of characteristic zero.
output: \( X_d^{r_1-1}(x) \) and \( Y_d^{r_1}(x) \) if \( X_d \) locally nilpotent.

Begin
\( p := \text{deg}_y(f) ; \)
\( H := H + \text{Quo}(\text{coeff}_x,c\text{oeff}_f,x) t^{d-1} ; \)
Else Return \( ([g]) ; \)
EndIf;
Else Return \( ([g]) ; \)
EndIf;
EndDo;
Else Return \( ([g]) ; \)
EndIf;
Return \( ([G,H]) ; \)
End;

The Algorithm RED

Input: Two polynomials \( f, g \) such that \( \text{deg}_y(f) \) divides \( \text{deg}_y(g) \).
output: A polynomial \( h \in \mathcal{A}[t] \) and \( \bar{g} \) of minimal degree such that \( g = h(f) + a \bar{g} \).

Begin
\( H := 0 ; G := g ; \)
If \( \text{divide}(\text{deg}(g,y),\text{deg}(f,y),d') \) and \( d \) integer Then
For \( i \) from 0 to \( d-1 \) Do
\( \text{coeff}_{x^i} := \text{coeff}(F,G,y,\text{deg}(f,y),(d-i)) ; \)
\( \text{coeff}_f := \text{coeff}(F,f^{d-i},y,\text{deg}(f,y),(d-i)) ; \)
If \( \text{Rem}(\text{coeff}_x,\text{coeff}_f,x) = 0 \) and \( \text{Quo}(\text{coeff}_x,\text{coeff}_f,x) \) is a polynomial Then
If \( \text{content}(\text{Quo}(\text{coeff}_x,\text{coeff}_f,x)) \) is integer Then
\( G := G - \text{Quo}(\text{coeff}_x,\text{coeff}_f,x) f^{d-1} ; \)
Else Return \( (g) ; \)
EndIf;
Else Return \( (g) ; \)
EndIf;
EndIf;
EndDo;
EndIf;
End;

The Algorithm LN
\( \ell := x \):

For \( i \) from 1 to \( p \)

While \( \deg_{(x,y)}(\ell) \neq 0 \) and \( \ell \neq 0 \)

\( g := \ell; \)

\( m := \partial_y f \partial_x (\ell) - \partial_x f \partial_y (\ell) \)

\( \ell := m; \)

If \( \deg_{(x,y)}(\ell) > \min(p(p - i), i(p - 2) + 1) \)

Then Return \( ([]) \);

EndIf:

EndDo:

\( k := y \):

For \( j \) from 1 to \( p \)

While \( \deg_{(x,y)}(k) \neq 0 \) and \( k \neq 0 \)

\( h := k; \)

\( n := \partial_y f \partial_x k - \partial_x f \partial_y k \)

\( k := n; \)

If \( \deg_{(x,y)}(k) > \min(p(p - j), j(p - 2) + 1) \)

Then Return \( ([]) \);

EndIf:

EndDo:

If \( \deg_{(x,y)}(\ell) = 0 \) and \( \ell \neq 0 \) and \( \deg_{(x,y)}(k) = 0 \) and \( k \neq 0 \)

Then Return \( ([y, \ell]) \);

Else Return \( ([]) \);

EndIf:

End:

6.2 Examples

For experimentation we have used the Computer Algebra System Maple (Release 7), under Windows on a P: III, 983MHz with 128 MB of memory.

1) Let us consider the first component of the well-known Nagata automorphism over \( \mathbb{Z}[x,y] \):

\[ f(x,y) := y + z^2x + zy^2. \]

By applying our algorithm, we find that it is a coordinate and that a coordinate's mate of minimum degree is

\[ g(x,y) := x - 2y + 2y^3 - z^3x^2 - 2z^2xy^2 - zy^4. \]

It is also of minimum degree over \( \mathbb{Q} \). Since \( \deg(g) > \deg(f) \), we deduce that The Nagata automorphism is not tame in \( \mathbb{Q}[x,y] \).

2) In the ring \( \mathbb{Z}[\sqrt{2}][x,y] \) we consider the polynomial defined by

\[ f(x,y) := x - 2y + \sqrt{2}(\sqrt{2}x - y^3) - \sqrt{2}(y - \sqrt{2}(\sqrt{2}x - y^3))^3. \]

Applying the algorithm we show that it is a coordinate and it has a mate of minimum degree

\[ g(x,y) := -y - \sqrt{2}y^2 + 2x. \]

3) Consider the polynomial in \( \mathbb{Z}[x,y] \) defined by

\[ f(x,y) := -z^2y^{12} + (3x^3 - 5z^4)y^9 + (3x^3 + 10z^4)y^9 + 5y + 3 + 3x^3 - 5z^3x^2. \]

Our algorithm shows that it is not a coordinate in \( \mathbb{Z}[x,y] \).

It is, however, a coordinate in the ring \( \mathbb{Q}[x,y] \), and a coordinate's mate is

\[ g(x,y) := -1/3z^2 - 1/5zy^4 + 1/5x. \]

4) In \( \mathbb{Z}[x,y] \) we consider the example given in [7] defined as

\[ f := y + z^2x^2 + 2z^3xy^2 + zy^3. \]

Our algorithm found that it is a coordinate and it’s computed mate is:

\[ g := 10z^7y^{17} + 20z^6xy^{18} + x + 280z^7x^2y^{13} + 120z^4xy^{12} + 80z^3xy^9 + 16z^2xy^6 + 20zy^5 + 90z^5x^2y^{16} + 80z^3xy^9 + 4z^4x^2y^6 + 2z^2y^{10} + 2z^2xy^6 + z^3x^2 + 2z^2xy^{10} + 420z^{12}x^4y^{12} + 420z^{16}x^8y^8 + 20z^{22}x^9y^9 + 90z^{40}x^2y^4 + 240z^{18}x^7y^6 + 120z^{12}x^5y^8 + 300z^{10}x^6y^6 + 400z^8x^3y^6 + 300z^6x^5y^8 + 20y^3z^9x^4 + 560z^9x^3y^{11} + 240z^{10}x^5y^2 + 10y^9 + 504z^4x^9y^{10} + 20y^2z^{13}x^8 + 700z^3x^7y^6 + 80z^{13}x^4y^9 + 280z^{18}x^5y^7 + 560z^{13}x^8y^7 + 80z^7x^5y + 120z^5x^7y^2 - 2z^3x^2y - 4xy^3 + 4z^3x^2y^2 + 9y^6. \]

7. REFERENCES


