Test of Monomorphism for Morphisms of Finite Type Between Affine Schemes

Sihem Mesnager

Institut de Mathématiques de Jussieu, Université de Paris VI
175 rue de Chevaleret, 75013 Paris, France
hachai@math.jussieu.fr

Abstract. In this paper, we give algorithmic criterion for morphisms of finite type between affine schemes to be a monomorphism. As side results, this paper also contains an algorithmic test for separability and an algorithmic criterion for "radiciality" in the sense of Grothendieck.

Introduction

Since the introduction of Grœbner bases, many authors have focused their interest on the construction of algorithms for testing properties of polynomial applications, encountered in classical algebraic geometry. An abbreviated list of such works is [2] [12] [15] [16] [4–7] [17].

In a preprint [4], written in 1986 but published only four years later in [5], van den Essen introduced for the first time the use of Gröbner bases to test invertibility of polynomial endomorphisms. In 1992, Kwiecinski [12] generalized van den Essen's result to test isomorphism between reduced algebras of finite type over a commutative field. This last result was again generalized by van den Essen in his last book [7], where he deals with the case of algebras of finite type over a commutative field. Shannon and Sweedler [16] used these same bases to test whether a given polynomial belongs to the image of a morphism between k-algebras of polynomials (k a field) of any dimension which so allow us to test the surjectivity and hence the bijectivity of such a morphism as well as its birationality. Ollivier [15] used Grœbner bases to test the injectivity of a polynomial mapping between two affine spaces with different dimension. In [6], van den Essen wrote algorithms allowing to decide whether a morphism between two affine varieties is finite, or, respectively, quasi-finite. From the test of quasi-finiteness, he deduced a test of flatness for a morphism of smooth varieties. Vasconcelos [17] also gave a test of flatness for certain algebras in particular for graded algebras and finitely generated algebras over a regular ring. Finally, Adjamagbo [2] recently proved how to decide whether a morphism of affine varieties is an open imbedding or not. Taking into account all the fore-cited works, we signal that the test of flatness has not been solved in the general case.

In this paper, we give algorithmic criterion for morphisms of finite type between affine schemes to be a monomorphism. This has been newer settled in the literature. As side results, this paper also contains an algorithmic test for separability and an algorithmic criterion for "radiciality" in the sense of Grothendieck. More precisely, given $\mathrm{Spec}(f) : \mathcal{Y} := \mathrm{Spec}(B) \to \mathcal{X} := \mathrm{Spec}(A)$ a morphism of finite type between K-affine schemes (where A and B are two finitely generated affine algebras over the same field K), we provide an algorithm to decide whether $\mathrm{Spec}(f)$ is a monomorphism of schemes or not, namely satisfies that : for any morphisms $g, h : \mathcal{Z} \to \mathcal{Y}$ (where $\mathcal{Z}$ is any affine scheme over K) , $f \circ g = f \circ h \Longrightarrow g = h$.

Grothendieck [10] gave a characterization of monomorphisms of schemes. He stated that a morphism of schemes is a monomorphism if and only if it is radiciel and its comorphism is unramified. In the case of affine schemes, a morphism between two affine schemes over a field K is unramified if and only if its comorphism is a separable morphism of K-algebras. Therefore, we first establish an algorithm to test the separability. To this end, we use the fact that the separability is equivalent to the existence of a left-inverse for a certain Jacobian matrix [18, 1]. Next, we establish an algorithm to test the property to be radiciel for morphism of finite type between K-affine schemes. To this end, we show that the property to be radiciel for $\mathrm{Spec}(f)$ is equivalent with the injectivity of the morphism obtained from $\mathrm{Spec}(f)$ by base change $\mathrm{Spec}(\bar{K}) \to \mathrm{Spec}(K)$ where $\bar{K}$ denotes an algebraic closure of K.

Notation. Throughout this paper, given a ring A, Spec(A) denotes the set of all prime ideals of A topologized by the Zariski topology.

1 Preliminaries

Throughout this section, A and B are rings which we assume to be commutative, with an identity. Let $\mathcal{X}$ and $\mathcal{Y}$ be affine schemes so that $\mathcal{X} := \mathrm{Spec}(A)$ and $\mathcal{Y} = \mathrm{Spec}(B)$. Let $\mathrm{Spec}(f) : \mathcal{Y} \to \mathcal{X}$ be a morphism of finite type so that it induces a homomorphism of rings $f : A \to B$. The homomorphism f makes B into an A-algebra. Let $B \otimes_A B$ be the tensor product of B with itself over A. Let π be the multiplication homomorphism from $B \otimes_A B$ to $B : \pi(b \otimes_A b') = bb'$ for all $(b, b') \in B^2$. We begin with introducing some definitions needed to express the characterizations of Grothendieck. The first definitions are the property of separability for two finitely generated algebras.

Definition 1. We say that B is a separable A-algebra if one of the following equivalent conditions is satisfied:

1. π induces on B a structure of projective $B \otimes_A B$-module.
2. The exact sequence
$$0 \to \ker \pi \to B \otimes_A B \xrightarrow{\pi} B \to 0$$
of $B \otimes_A B$-modules splits (where B is endowed with its $B \otimes B$-module structure induced by π).
3. There exists an element idempotent e in $B \otimes_A B$ such that $\pi(e) = 1$ and $(\ker \pi)\, e = \{0\}$ (or also $\pi(e) = 1$ and $e(b \otimes 1) = e(1 \otimes b)$ for all $b \in B$).

Example 2. The homomorphism $f : \mathbb{F}_p[X] \to \mathbb{F}_p[Y]$ which maps X to $Y^p + Y$ ($\mathbb{F}_p$ stands for the finite field with prime characteristic p) is separable. On the other hand, the homomorphism $f' : \mathbb{F}_p[X] \to \mathbb{F}_p[Y]$ which maps X to Y^p (associated to the Frœbenius morphism $\bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$ which maps x to x^p) is not separable.

Next we define the property to be unramified.

Definition 3. We say that B is a unramified A-algebra if and only if B is a separable A-algebra and $\ker \pi$ is a finitely generated ideal of $B \otimes_A B$.

Remark 4. When B is a finitely generated A-algebra (up to an isomorphism), the condition on $\ker \pi$ in the definition 3 is always fulfilled and thus we have

$$B \text{ is an unramified } A\text{-algebra} \iff B \text{ is a separable } A\text{-algebra}$$

Next we recall the notion of *radiciel* morphism [10].

Definition 5. A morphism of schemes $f : \mathcal{X} \to \mathcal{Y}$ is said to be radiciel if f is universally injective, i.e. for every $\mathcal{Y}' \to \mathcal{Y}$, the morphism $f' : \mathcal{X}' \to \mathcal{Y}'$ obtained from f by base change is injective.

We now state some characterizations of radiciel morphisms which shall help us in our study.

Proposition 6. *Let $f : \mathcal{X} \to \mathcal{Y}$ be a morphism of schemes. Then the below assertions are equivalent*

1. *f is radiciel.*
2. *For any field K', the map $f(K') : \mathcal{Y}(K') \to \mathcal{X}(K')$ is injective where $\mathcal{X}(K')$ (*resp. *$\mathcal{Y}(K')$) denotes* $\mathrm{Hom}(K', \mathcal{X})$ (resp. $\mathrm{Hom}(K', \mathcal{Y})$), i.e *the set of all morphisms from K' to $\mathcal{X}$ (*resp. *$\mathcal{Y}$).*
3. *The diagonal morphism $\Delta_f : \mathcal{Y} \to \mathcal{Y} \times_{\mathcal{X}} \mathcal{Y}$ is onto (where $\mathcal{Y} \times_{\mathcal{X}} \mathcal{Y}$ denotes the fiber product of $\mathcal{X}$-schemes)*

Example 7. The frœbenius morphism $f : \overline{\mathbb{F}}_p \longrightarrow \mathbb{F}_p$ which maps x to x^p defined on the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ is radiciel.

Example 8. The $\mathbb{R}$-morphism of schemes $f : \mathrm{Spec}(\mathbb{C}) = \mathrm{Spec}\left(\mathbb{R}[t]/(t^2+1)\right) \to \mathrm{Spec}(\mathbb{R})$ is injective but not radiciel. Indeed, the $\mathbb{C}$-morphism of schemes $\mathrm{Spec}(\mathbb{C}[t]/(t^2+1)) \to \mathrm{Spec}(\mathbb{C})$ obtained from f by base change $\mathrm{Spec}(\mathbb{C}) \to \mathrm{Spec}(\mathbb{R})$ is not injective.

Grothendieck [10] stated the below characterization of monomorphism

Theorem 9. *Let $\mathcal{X}$ and $\mathcal{Y}$ be affine schemes and let $\mathrm{Spec}(f) : \mathcal{Y} \to \mathcal{X}$ of schemes. Then f is a monomorphism if and only if it is radiciel and its comorphism is unramified.*

Using remark 4, we reformulate the above characterization as

Corollary 10. *Let A and B be two finitely generated K-algebras (where K is any commutative field). The morphism of affine schemes $\mathrm{Spec}(f) : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ is a monomorphism if and only if the morphism $\mathrm{Spec}(f)$ is radiciel and its comorphism $f : A \longrightarrow B$ is separable.*

2 Test of Monomorphism for Morphism Between Affine Schemes over the Same Field

In this section, we base on Corollary 10 and provide a computational method to decide whether or not a morphism $\mathrm{Spec}(f) : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$, where A and B are finitely generated algebras over the same field K, is a monomorphism or not. We first establish a test of separability in subsection 2.1 using a Jacobian criterion of separability taken from [1]. Next, we show how to reduce the problem of testing if $\mathrm{Spec}(f)$ is radiciel to test if the morphism obtained from $\mathrm{Spec}(f)$ by base change $\mathrm{Spec}(\bar{K}) \to \mathrm{Spec}(K)$ is injective. This leads us to a computational test for "radiciality" exposed in Proposition 15.

Let K be a commutative field. Let $K[X]$ (*resp.* $K[Y]$) the K-algebra of polynomials generated by a system $X := (X_1, ..., X_n)$ (*resp.* $Y := (Y_1, ..., Y_m)$) of indeterminates over R. Let P_1, ..., P_r (resp Q_1, ...,Q_s) elements of $K[X]$ (resp. $K[Y]$). Set $A := K[X]/\sum_{i=1}^{r} P_i K[X] = K[x_1, ..., x_n]$ where $x_j = X_j + \sum_{i=1}^{r} P_i K[X]$ for $1 \leq j \leq n$ and $B := K[Y]/\sum_{i=1}^{s} Q_i K[Y] = K[y_1, ..., y_m]$ where $y_j = Y_j + \sum_{i=1}^{s} Q_i K[X]$ for $1 \leq j \leq m$. Consider a homomorphism f between K-algebras from A to B defined as $f\left(X_j + \sum_{i=1}^{r} P_i K[X]\right) = F_j + \sum_{i=1}^{s} Q_i K[Y]$ with $F_j \in K[Y]$ for $1 \leq j \leq n$.

We finally introduce some miscellaneous notation needed to express our results. We denote δ_{ij} the Kronecker symbol : $\delta_{ii} = 1$ and $\delta_{ij} = 0$ if $i \neq j$; given a vector, we add a superscript of the form (i) to indicate the i-th component of this vector; we put a superscript ^{t} before to denote the transpose matrix.

2.1 Test of Separability

Although there exists other necessary and sufficient criterions for characterizing the separability for two finitely presented algebras, we put emphasis, with the aim of a computational use, on the criterion known by the name of Jacobian criterion for separability given by Wang [18]. He considered $B := A[T_1, ..., T_n]/(h_i)_{i \in I}$ (T_1, ..., T_n are indeterminates over A, I is a finite set of indices and h_i, $i \in I$, are polynomials in $A[T_1, ..., T_n]$. He proved that the separability of B over A is equivalent to the existence of a row-finite left-inverse in B for the Jacobian matrix of relations. This criterion has been reworded for finitely presented algebras in [2]. The statement in [2] relies on the Jacobian matrix of $(F_1, ..., F_n, Q_1, ..., Q_s)$ with respect to Y

$$\mathcal{J}_Y(F,Q) := \begin{pmatrix} \frac{\partial F_1}{\partial Y_1} & \cdots & \frac{\partial F_1}{\partial Y_m} \\ \vdots & & \vdots \\ \frac{\partial F_n}{\partial Y_1} & \cdots & \frac{\partial F_n}{\partial Y_m} \\ \frac{\partial Q_1}{\partial Y_1} & \cdots & \frac{\partial Q_1}{\partial Y_m} \\ \vdots & & \vdots \\ \frac{\partial Q_s}{\partial Y_1} & \cdots & \frac{\partial Q_s}{\partial Y_m} \end{pmatrix} \quad (1)$$

The criterion of separability for two finitely presented algebras exposed in [2] is then

Proposition 11. *The following assertions are equivalent*

1. *The A-algebra B induced by f is separable.*
2. *$m \leq n+s$ and the canonical image in $\mathcal{M}_{n+s,m}(B)$ of $\mathcal{J}_Y(F,Q)$ is left-invertible.*

Proposition 11 thus connects the separability of B over A to the left-invertibility of the canonical image in $\mathcal{M}_{n+s,m}(B)$ of $\mathcal{J}_Y(F,Q)$. We are thus brought to establish a computational criterion to decide if the canonical image in $\mathcal{M}_{n+s,m}(B)$ of $\mathcal{J}_Y(F,Q)$ is left-invertible or not. Before, we introduce the notion of *syzygy* module of a matrix : Let M be a matrix in $\mathcal{M}_{pq}(K[Y_1, ..., Y_m])$; Denote C_1, ..., C_q the columns of M; The syzygy module of M is the set of all $(a_1, ..., a_q) \in (K[Y_1, ..., Y_m])^q$ such that $a_1C_1 + ... + a_qC_q = 0$; It is a $K[Y_1, ..., Y_m]$-submodule of $(K[Y_1, ..., Y_m])^q$ and is denoted $\mathrm{syz}(M)$.

Proposition 12. *Let $<$ be a term order on $K[Y_1, ..., Y_m]$. Let $\{H_1, ..., H_w\}$ be a generating set of the syzygy $K[Y_1, ..., Y_m]$-submodule of $(K[Y_1, ..., Y_m])^{m(n+s)+m^2s+1}$ of the $m^2 \times m(n+s)+m^2s+1$-matrix*

$$\left(\begin{array}{c:c:c:c:c:c:c} {}^t\mathcal{J}_Y(F,Q) & 0 & 0 & \begin{matrix}-\delta_{11}\\ \vdots \\ -\delta_{1m}\end{matrix} & Q_1 \ \dots \ Q_s & & 0 \\ \hdashline 0 & \ddots & 0 & \vdots & 0 & \ddots & 0 \\ \hdashline 0 & 0 & {}^t\mathcal{J}_Y(F,Q) & \begin{matrix}-\delta_{m1}\\ \vdots \\ -\delta_{mm}\end{matrix} & 0 & & Q_1 \ \dots \ Q_s \end{array}\right) \quad (2)$$

Then, B is a separable A-algebra if and only if

$$1 \in \sum_{i=1}^{w} H_i^{(m(n+s)+1)} K[Y]$$

Proof. According to Proposition 11, the separability of B over A as A-algebra is equivalent to the existence of a row-finite left-inverse of the canonical image $\bar{\mathcal{J}}_Y(F,Q)$ in $\mathcal{M}_{n+s,m}(B)$ of the

Jacobian matrix $\mathcal{J}_Y(F,Q)$ given by (1). Now, by definition, the matrix $\bar{\mathcal{J}}_Y(F,Q)$ is left-invertible if and only if there exists a matrix $\bar{\mathcal{K}}_Y(F,Q) \in \mathcal{M}_{m,n+s}(B)$ such that

$$\bar{\mathcal{K}}_Y(F,Q)\,\bar{\mathcal{J}}_Y(F,Q) \;=\; \bar{\mathrm{I}}_m$$

where $\bar{\mathrm{I}}_m$ denotes the identity matrix of $\mathcal{M}_m(B)$. This is equivalent to

$$^t\bar{\mathcal{J}}_Y(F,Q)\,{}^t\bar{\mathcal{K}}_Y(F,Q) \;=\; \bar{\mathrm{I}}_m \tag{3}$$

Denote then $\bar{C}_1$, ..., $\bar{C}_m$ the columns of $\bar{\mathrm{I}}_m$ and $\bar{\zeta}_1$, ..., $\bar{\zeta}_m$ the columns of ${}^t\bar{\mathcal{K}}_Y(F,Q)$. Then (3) can be reformulated as

$$\forall i \in \{1,...,m\}, \quad {}^t\bar{\mathcal{J}}_Y(F,Q)\,\bar{\zeta}_i \;=\; \bar{C}_i \tag{4}$$

or in block-matrix form

$$\left(\begin{array}{c|c|c} {}^t\bar{\mathcal{J}}_Y(F,Q) & 0 & 0 \\ \hline 0 & \ddots & 0 \\ \hline 0 & 0 & {}^t\bar{\mathcal{J}}_Y(F,Q) \end{array}\right) \begin{pmatrix} \bar{\zeta}_1 \\ \vdots \\ \vdots \\ \vdots \\ \bar{\zeta}_m \end{pmatrix} = \begin{pmatrix} \bar{C}_1 \\ \vdots \\ \vdots \\ \vdots \\ \bar{C}_m \end{pmatrix} \tag{5}$$

This latter system is equivalent to say that there exists α_1, ..., $\alpha_{m^2(n+s)}$ in $K[Y]$ such that

$$N \begin{pmatrix} \zeta_1 \\ \vdots \\ \zeta_m \\ 1 \\ \alpha_1 \\ \vdots \\ \alpha_{m^2(n+s)} \end{pmatrix} = 0 \iff ({}^t\zeta_1, ..., {}^t\zeta_m, \underset{\substack{\uparrow \\ (m(n+s)+1)\text{th-coordinate}}}{1}, \alpha_1, ..., \alpha_{m^2(n+s)}) \in \mathrm{syz}(N)$$

where N is the matrix of $\mathcal{M}_{m^2, m(n+s)+1+m^2(n+s)}(K[Y_1, ..., Y_m])$ defined by (2). Let $\{H_1, ..., H_w\}$ be a generating set of the syzygy $K[Y_1, ..., Y_m]$-submodule of $(K[Y_1, ..., Y_m])^{m(n+s)+1+m^2(n+s)}$ of the matrix N. Then, we can conclude that $\bar{\mathcal{J}}_Y(F,Q)$ is left-invertible if the ideal generated by the $(m(n+s)+1)$th-coordinates of the elements of $\{H_1, ..., H_w\}$ contains 1.

2.2 A Test of Universal Injectivity

First of all, we show that the problem of deciding whether the morphism Spec(f) is radiciel or not can be reduced to test the injectivity of the morphism obtained from Spec(f) be base change Spec$(\bar{K}) \longrightarrow$ Spec(K).

Proposition 13. *Let K be a commutative field. Let $\bar{K}$ be an algebraic closure of K. Let $\mathcal{X}$ and $\mathcal{Y}$ be K-affine schemes of finite type. Let* Spec(f) : $\mathcal{Y} \longrightarrow \mathcal{X}$ *be a morphism of finite type. Let* u : Spec$(\bar{K}) \longrightarrow$ Spec(K) *be a base change. Denote $\tilde{f}' : \mathcal{Y}' \longrightarrow \mathcal{X}'$ the morphism of $\bar{K}$-affine schemes obtained from* Spec(f) *by the base change u. Then*

$$(\mathrm{Spec}(f) \textit{ is radiciel}) \iff \left(\tilde{f}' \textit{ is injective}\right) \tag{6}$$

Proof. Firstly, note that it suffices to show the below equivalence to show (6).

$$\left(\tilde{f}' \text{ is radiciel}\right) \Leftrightarrow \left(\tilde{f}' \text{ is injective}\right) \tag{7}$$

Indeed, if $\tilde{f}'$ is injective then, according to (7), $\tilde{f}$ is radiciel. Now, since the base change u : Spec$(\bar{K}) \to$ Spec(K) is onto, [10, proposition 26.1 p. 27] states that if $\tilde{f}'$ is radiciel then Spec(f)

est radiciel. Conversely, the definition of the property to be radiciel means that if $\mathrm{Spec}(f)$ is radiciel, then any morphism obtained from $\mathrm{Spec}(f)$ by base change is injective. Thus, in particular, $\tilde{f}'$ is injective.

Let us now show (7). Clearly, a radiciel morphism is in particular injective. We hence only need to show that if $\tilde{f}'$ is injective then $\tilde{f}'$ is radiciel. Assume from now on that $\tilde{f}'$ is injective. We then show show to that the diagonal morphism $\Delta_{\tilde{f}'} : \mathcal{Y}' \to \mathcal{Y}' \times_{\mathcal{X}'} \mathcal{Y}'$ is onto which implies that $\tilde{f}'$ is radiciel according to proposition 6.

Under the terms of [11, corollary 3.6.3 p. 245], it suffices to show that, for any extension K' of $\bar{K}$, the map $\Delta_{\tilde{f}'(K')} : \mathcal{Y}'(K') \to \mathcal{Y}' \times_{\mathcal{X}'} \mathcal{Y}'(K')$ inducted by $\Delta_{\tilde{f}'}$ is onto. Let K' be any extension of $\bar{K}$. Since $\tilde{f}'$ is a morphism of affine schemes and according to [11, proposition 5.2.2 p. 277], $\tilde{f}'$ is separated, *i.e.* its diagonal $\Delta_{\tilde{f}'}$ is a closed subscheme of $\mathcal{Y}' \times_{\mathcal{X}'} \mathcal{Y}'$. Now, $\tilde{f}$ is a morphism of finite type, the complement of the image of the diagonal $\Delta_{\tilde{f}'(K')}$ relative to the product $\mathcal{Y}' \times_{\mathcal{X}'} \mathcal{Y}'(K')$ has then a structure of open $\bar{K}$-subscheme of $\mathcal{Y}' \times_{\mathcal{X}'} \mathcal{Y}'(K')$. Moreover, since the morphism $\tilde{f}'$ is injective, the map $\tilde{f}'(\bar{K}) : \mathcal{Y}'(\bar{K}) \to \mathcal{X}'(\bar{K})$ is injective. Therefore, the diagonal map $\Delta_{\tilde{f}'(\bar{K})} : \mathcal{Y}'(\bar{K}) \to \mathcal{Y}' \times_{\mathcal{X}'} \mathcal{Y}'(\bar{K}) = \mathcal{Y}'(\bar{K}) \times_{\mathcal{X}'(\bar{K})} \mathcal{Y}'(\bar{K})$ is onto which is equivalent to say that the complement of the image of the diagonal $\Delta_{\tilde{f}'(\bar{K})}$ relative to the product $\mathcal{Y}' \times_{\mathcal{X}'} \mathcal{Y}'(\bar{K})$ is empty. Hence, the complement of the image of the diagonal $\Delta_{\tilde{f}'(K')}$ is an open $\bar{K}$-subscheme which has no points on $\bar{K}$. The Hilbert Nullstellensatz ensures that this open set is empty. Therefore, $\Delta_{\tilde{f}'(K')}$ is onto and thus $\tilde{f}'$ is radiciel which completes the proof.

Before stating our test of universal injectivity, we recall first the following helpful result exposed in [3]

Proposition 14. *Let K be a commutative field. Let I be the ideal of $K[X_1, ..., X_n]$ generated by the polynomials f_1, ..., f_s of $K[X_1, ..., X_n]$. Let $f \in K[X_1, ..., X_n]$. Let Y be another indeterminate over K and let $\tilde{I}$ be the ideal of $K[X_1, ..., X_n, Y]$ generated by f_1, ..., f_s and $1 - Yf$. Then $f \in \sqrt{I}$ if and only if $1 \in \tilde{I}$.*

We then establish the below computational criterion based on Grœbner basis to decide if $\mathrm{Spec}(f)$ is radiciel or not

Proposition 15. *Let Z_1, ..., Z_m and W be new indeterminates over $\bar{K}$. Let $<$ be an admissible term order on $\bar{K}[Y, Z, W] := \bar{K}[Y_1, ..., Y_m, Z_1, ..., Z_m, W]$. For each $i \in \{1, ..., m\}$, denote $\mathcal{D}_i$ the ideal of $\bar{K}[Y, Z, W]$ generated by the polynomials $F_1(Y) - F_1(Z)$, $\dots$, $F_n(Y) - F_n(Z)$, $Q_1(Y)$, $\dots$, $Q_s(Y)$, $Q_1(Z)$, $\dots$, $Q_s(Z)$ and $1 - W(Y_i - Z_i)$.*

Then $\mathrm{Spec}(f)$ *is radiciel if and only if, for each $i \in \{1, ..., m\}$, the reduced grœbner basis of $\mathcal{D}_i$ with respect to $<$ is equal to $\{1\}$.*

Proof. Let $\tilde{f}' : \mathcal{X}' := \mathrm{Spec}(B) \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\bar{K}) \to \mathcal{Y}' := \mathrm{Spec}(A) \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\bar{K})$ be the morphism of $\bar{K}$-affine scheme obtained from $\mathrm{Spec}(f)$ by the base change $\mathrm{Spec}(\bar{K}) \to \mathrm{Spec}(K)$. Proposition 13 connects the problem of testing that f is radiciel to test the injectivity of $\tilde{f}'$. By definition, $\tilde{f}'$ is injective if and only if, whenever $(y_1, ..., y_m) \in \bar{K}^m$ and $(z_1, ..., z_m) \in \bar{K}^m$ and $\tilde{f}'(y_1, ..., y_m) = \tilde{f}'(z_1, ..., z_m)$, it always turns out that $(y_1, ..., y_m) = (z_1, ..., z_m)$. Note now

$$\begin{aligned}\mathrm{Spec}(A) \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\bar{K}) &= \mathrm{Spec}\left(A \otimes_K \bar{K}\right)\\ &= \mathrm{Spec}\left(\bar{K}[X_1, ..., X_n] / \sum_{i=1}^{r} P_i \bar{K}[X_1, ..., X_n]\right)\end{aligned}$$

and

$$\begin{aligned}\mathrm{Spec}(B) \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\bar{K}) &= \mathrm{Spec}\left(B \otimes_K \bar{K}\right)\\ &= \mathrm{Spec}\left(\bar{K}[Y_1, ..., Y_m] / \sum_{i=1}^{s} Q_i \bar{K}[Y_1, ..., Y_m]\right)\end{aligned}$$

Let $\bar{I}$ be the ideal of $\bar{K}[Y_1, ..., Y_m, Z_1, ..., Z_m]$ generated by all the polynomials $F_1(Y_1, ..., Y_m) - F_1(Z_1, ..., Z_m)$, ..., $F_n(Y_1, ..., Y_m) - F_n(Z_1, ..., Z_m)$, $Q_1(Y_1, ..., Y_m)$, ..., $Q_s(Y_1, ..., Y_m)$, $Q_1(Z_1, ..., Z_m)$,

..., $Q_s(Z_1, ..., Z_m)$ and let $\bar{J}$ be the ideal of $K[Y_1, ..., Y_m, Z_1, ..., Z_m]$ which generators are $Y_1 - Z_1$, ..., $Y_m - Z_m$. Denote then $\mathcal{V}(\bar{I})$ and $\mathcal{V}(\bar{J})$ the varieties of $\bar{K}^{2m}$ defined, respectively, by the ideals $\bar{I}$ and $\bar{J}$. Then

$$\tilde{f}' \text{ is injective} \Leftrightarrow \mathcal{V}(\bar{I}) \subset \mathcal{V}(\bar{J}) \Leftrightarrow \sqrt{\bar{I}} \supset \sqrt{\bar{J}} \Rightarrow \sqrt{\bar{I}} \supset \bar{J}$$

(by Nullstellensatz theorem, $\bar{K}$ being algebraically closed). Conversely, if $\sqrt{\bar{I}} \supset \bar{J}$ then $\sqrt{\bar{J}} \subset \sqrt{\bar{I}}$. Therefore, $\tilde{f}'$ is injective if and only if $\sqrt{\bar{I}} \supset \bar{J}$, namely, if and only if $Y_i - Z_i \in \sqrt{\bar{I}}$ for every $i \in \{1, ..., m\}$. Now, according to Proposition 14, say that $Y_i - Z_i \in \sqrt{\bar{I}}$ for every $i \in \{1, ..., m\}$ is equivalent to say that, for every $i \in \{1, ..., m\}$, 1 belongs to the ideal of $\bar{K}[Y_1, ..., Y_m, Z_1, ..., Z_m, W]$ generated by the generators of $\bar{I}$ and by $1 - W(Y_i - Z_i)$.

2.3 Algorithm

We provide in this section an algorithm based on Proposition 12 and Proposition 15 to test whether a finitely generated morphism of affine schemes is a monomorphism or not. For the sake of clarity, we begin with an algorithm written in pseudo-computer style.

Algorithm 16 IsMonomorphism $\mathrm{Spec}(f) : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$

Require: $m \leq n + s$.
  Let N be the matrix of $\mathcal{M}_{m^2, m(n+s)+m^2 s+1}(K[Y])$ defined by (2).
  Compute a generating set G of the syzygy $K[Y_1, ..., Y_m]$-submodule of $(K[Y_1, ..., Y_m])^{m(n+s)+m^2 s+1}$ of N.
  if $1 \notin G$ **then**
    Return Spec(f) is not a monomorphism.
  else
    Let $G = \{1\}$.
    Let $i = 1$.
    while $G = \{1\}$ **do**
      Compute a reduced Grœbner basis G of $\mathcal{D}_i$ with respect to an admissible term order (where $\mathcal{D}_i$ denotes the ideal defined in the body of proposition 15)
      Let $i = i + 1$
    end while
    if $G = \{1\}$ **then**
      Return Spec(f) is a monomorphism.
    else
      Return Spec(f) is not a monomorphism.
    end if
  end if

Assume $m = 1$, $n = 2$, $r = 1$, $s = 0$, $P_1(X_1, X_2) = X_1^3 - X_2^3$, $F_1(Y_1) := Y_1$, $F_1(Y_1) = Y_1^2$. We assume that $K = \mathbb{Q}$. In order to illustrate our algorithm, we check that the morphism of K-schemes $f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is an monomorphism or not. Throughout this example, we use the Computer Algebra system Singular [8, 9] and we adopt the following typographical conventions : text in `typewriter` denotes Singular input and output (moreover, we add an arrow `->` to specify Singular output). We provide first an implementation of algorithm 16 in the computer algebra system Singular :

```
proc IsMonomorphism(map f)
{
string Current=nameof(basering);
int m=nvars(basering);
int n=size(ideal(f));
if (typeof(basering)=="qring")
{ideal Q=ideal(basering); int s=size(Q);} else
```

```
{ ideal Q=ideal(0); int s=0; }
if (m<=n+s)
{
int i;
int j;
matrix jac[n+s][m];
for (i=1;i<=n;i++) {for(j=1;j<=m;j++) {
                         jac[i,j]=diff(f[i],var(j));}}
for (i=1;i<=s;i++) {for(j=1;j<=m;j++) {
                         jac[n+i,j]=diff(f[i],var(j));}}
matrix N[m^2][m*(n+s)+1];
for (i=1;i<=m;i++) {N[(i-1)*m+1..i*m,(i-1)*(n+s)+1..i*(n+s)]=transpose(jac);}
N[1..m*m,m*(n+s)+1]=-unitmat(m);
for (i=1;i<=s;i++) {N=concat(N,Q[i]*unitmat(m*m));}
matrix H=syz(N);
if (reduce(poly(1),std(ideal(H[m*(n+s)+1,1..ncols(H)])))==poly(0))
{
extendring("C",m+1,"Z(","lp",1,basering);
i=1;
execute("map g=fetch("+Current+",f)");
execute("map phi=C,Z(1.."+string(m)+");");
execute("ideal Q2=fetch("+Current+",Q)");
ideal I=ideal(g);
if (s==0) {ideal J=I-phi(I);} else {ideal J=I-phi(I),Q2,phi(Q2);}
ideal K;
int ok=1;
while ((i<=m) and (ok==1))
{
ok=(reduce(poly(1),groebner(J+ideal(1-var(2*m+1)*(var(i)-var(m+i)))))==poly(0));
i=i+1;
}
if (ok==1) {return (1);} else {return (0);} } else { return (0); } } else
{
return (0);
}
execute("keepring "+Current);
}
```

Note. The above procedure returns the integer values 0 and 1 which represent the boolean values FALSE and TRUE.

Then, we check thanks to this procedure that f is a monomorphism of schemes.

```
LIB "matrix.lib";
option(redSB);
ring R=0,(X(1..2)),lp;
qring A=std(X(1)^3-X(2)^3);
ring B=0,Y(1),lp;
map f=A,Y(1)^2,Y(1);
IsMonomorphism(f);
-> 1 /* f is a monomorphism */
```

References

1. Adjamagbo, K.: On Separable algebras over a U.F.D and the Jacobian conjectures in any characteristic. Prépublication de l'Institut de Mathématiques de Jussieu - Université Paris VI (1995).

2. Adjamagbo, K.: Test of open immersion for morphisms of affine algebraic varieties, 18-22 Septembre 2000. Kraków, Effective methods in algebraic and analytic geometry III (2000).
3. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties and Algorithms. Springer-Verlag, (1991).
4. van den Essen, A. : A criterion to decide if a polynomial map is invertible and compute the inverse. Technical Report 8653, University of Nijmegen (1986).
5. van den Essen, A.: A criterion to decide if a polynomial map is invertible and compute the inverse. Comm. in algebra, 18(10) (1990), 3183-3186.
6. van den Essen, A.: Algorithms for deciding finiteness and quasi-finiteness of morphims between algebraic varieties and an application to flatness. Technical Report 9559, Department of Mathematics - University of Nijmegen - Netherlands (1995).
7. van den Essen, A.: Polynomial Automorphisms and the Jacobian conjecture, volume 190 of *Progress in Mathematics*. Birkhaser,(2000).
8. Greuel, G.M., Pfister, G., Schönemann, H.: SINGULAR 2.0.4, Centre for Computer Algebra, A Computer Algebra System for Polynomial Computations, University of Kaiserslautern, `http://www.singular.uni-kl.de` (2001)
9. Greuel, G.M., Pfister, G. : A SINGULAR introduction to commutative algebra, Algorithms and computations in Mathematics, 10, Springer-Verlag (2002).
10. Grothendieck, A.: Eléments de Géométrie Algébrique. Volume IV, quatrième partie (1966).
11. Grothendieck, A., Dieudonné, J.A.: Eléments de Géométrie Algébrique. Volume I, Springer-Verlag (1971).
12. Kwiecinski, M.: A Grœbner basis criterion for isomorphisms of algebraic varieties. J. of pure and Applied Algebra, 74 (1991), 275-279 .
13. Mesnager, S.: Contributions à l'étude effective de morphismes de schémas affines. PhD thesis, Université de Paris VI (2002).
14. Mesnager, S.: Test of epimorphism for finitely generated morphisms between affine algebras, submitted.
15. Ollivier, F.: Le problème de l'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité. PhD thesis, Ecole Polytechnique (1990).
16. Shannon, D., Sweedler, M.: Using Gröbner bases to determine algebra membership, split surjective algebra homomorphisms, determine birational equivalence. J. Symb. Comp., 6 (1988), 267-273.
17. Vasconcelos, V.W.: Computational Methods in Commutative Algebra and Algebraic Geometry. Springer (1997).
18. Wang, S.S.: A Jacobian criterion for separability. J. of Algebra, 65 (1980), 453-494.