Inversibility of Rational Mappings and Structural Identifiability in Automatics

François Ollivier

Laboratoire d'Informatique de l'X (LIX)
École Polytechnique
F-91128 Palaiseau Cedex (France)
BITNET: CFFOLL@FRPOLY11
uucp: ollivier@cmep.polytechnique.fr

February, 3rd 1994

Abstract: We investigate different methods for testing whether a rational mapping f from k^n to k^m admits a rational inverse, or whether a polynomial mapping admits a polynomial one. We give a new solution, which seems much more efficient in practice than previously known ones using "tag" variables and standard basis, and a majoration for the degree of the standard basis calculations which is valid for both methods in the case of a polynomial map which is birational. We further show that a better bound can be given for our method, under some assumption on the form of f. Our method can also extend to check whether a given polynomial belong to the subfield generated by a finite set of fractions.

We then illustrate our algorithm, with a application to structural identifiability. The implantation has been done in the IBM computer algebra system Scratchpad II.

0. Introduction

It is already known that such questions as testing whether a given polynomial Q belongs to $k[P_1, \ldots, P_m]$ can be solved by considering the reduction of Q with respect to the standard basis of the ideal $(P_i - T_i)$ in $k[X_1, \ldots, X_n, T_1, \ldots, T_m]$ for an ordering which eliminates $X_1, \ldots, X_n$. The technique of using m "tag" variables is attributed to Spear by David Shannon and Moss Sweedler, who made an important work to apply it for testing membership to a finite subalgebra of a polynomial ring (see [SS1]), or of a field of fractions (see [SS2]).

Such a method can be used to test if $k[P_1, \ldots, P_m]$ is equal to $k[X_1, \ldots, X_n]$, which means that the polynomial map from k^n to k^m defined by the P_i admits a polynomial inverse. Shannon and Sweedler apply it also for testing whether the field of fractions $k(P_1, \ldots, P_n)$ is equal to $k(X_1, \ldots, X_n)$. In that case, the associated mapping is birational.

We will extend this result in ordering to get a similar one in the case of m rational fractions. We then prove in the birational case and for f polynomial a majoration on the degree of polynomials calculated during a standard basis computation, relying on a result of O. Gabber.

Our interest on this problems was originated by the problem of structural identifiability. It led us to investigate practical tests of inversibility for rational mappings, without caring much for an expression of the inverse. We were greatly influenced by preceding works by E. Walter, Y. Lecourtier and A. Raksanyi who applied computer algebra to the study of structural properties in automatics (see [L], [R] or [LW]). They already used only n additional variables in the same way as we do. But their method relies on pseudo-divisions and is therefore related to Wu's one, which is not the most efficient in our case.

We show our method rely on a more precise result, which could be used to test whether a given fraction belongs to the subfield generated by a finite set of fractions. The ideal we associate to a subfield does not depend on the set of generators chosen. Furthermore, the preceding bound is still valid and a better one can be obtained under some assumptions always verified in all the applications we have done so far.

Our method is still valid to test the existence of a polynomial inverse if $n = m$. Howether it cannot be used to answer the membership problem for $k[P_1, \ldots, P_m]$.

The last part is devoted to applications, mostly to structural identifiability. We show here briefly how it can be reduced to an algebraic problem and then describe the algorithm as implemented in SCRATCHPAD. Two examples are then given, one of them being unsolved by RAKSANYI's algorithm.

The last example show the efficiency in a purely rational case, where the extended tag variable method does not succeed.

1. Testing Inversibility with Standard Basis and Tag Variables

We will allow ourselves bellow, where no confusion can be done to write x^α for $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, $k[x]$ for $k[x_1, \ldots, x_n]$ and $k(\frac{P}{Q})$ for $k(\frac{P_1}{Q_1}, \ldots, \frac{P_m}{Q_m})$.

1.1. The Polynomial Case

We consider a polynomial mapping

$$\begin{array}{rcccl} f & : & k^n & \longrightarrow & k^n \\ & & (x_1, \ldots, x_n) & \longrightarrow & (P_1(x_1, \ldots, x_n), \ldots, P_m(x_1, \ldots, x_n)) \end{array}$$

where k is any field, and want to test whether it admits a polynomial inverse. It is obviously equivalent to test that $k[P_1, \ldots, P_m]$ is equal to $k[X_1, \ldots, X_n]$. So we will first investigate how the membership problem for a finite k-subalgebra can be solved. the method we give here is from SHANNON and SWEEDLER (see [SS1]).

We give ourselves m additional "tag" variables $t_1, \ldots, t_m$, and consider the ideal $\mathcal{I}$ generated by the m polynomials $P_i - t_i$ in $k[x_1, \ldots, x_n, t_1, \ldots, t_m]$. As it is the kernel of the ring homomorphism

$$\begin{array}{rcccl} G & : & k[x_1, \ldots, x_n, t_1, \ldots, t_m] & \longrightarrow & k[x_1, \ldots, x_n] \\ & & x_i & \longrightarrow & x_i \\ & & t_j & \longrightarrow & P_j, \end{array}$$

$\mathcal{I}$ is prime. We will show that the reduced standard basis of $\mathcal{I}$ with respect to some admissible orderings can be used to answer the membership problem.

DEFINITION 1. The admissible ordering $\prec$ on monomials of $k[x_1, \ldots, x_n, t_1, \ldots, t_m]$ is said to *eliminate globally* $x_1, \ldots, x_n$ if for any two monomials $m_1 = x^\alpha$ and $m_2 = x^\beta$,

$$\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \Rightarrow m_1 \prec m_2.$$

It is well known that for such an ordering, the set of polynomials in the standard basis of any ideal $\mathcal{J}$ whose leading term depends only of the t_i form a standard basis of $\mathcal{J} \cap k[t]$. they obviously are in $k[t]$ for the total degree in x of any of their monomials must be equal or less than the one of the leading monomial, and so 0.

PROPOSITION 1. *Calling ST the standard basis of the ideal $\mathcal{I}$, defined as above, for any admissible ordering $\prec$ which eliminates globally $x_1, \ldots, x_n$, and Q being any polynomial of $k[x]$ the two following properties are equivalent:*

(i) Q belongs to $k[P]$,

(ii) the reduction of Q with respect to ST belongs to $k[t]$.

Moreover, if Q is in $k[P]$, the reduction of Q gives the expression of Q in function of $P_1, \ldots, P_m$.

PROOF. ($\Rightarrow$) $\mathcal{I}$ being the kernel of G, for any polynomial Q in $k[P]$, say $Q = R(P)$, $R(P) - R(t) = Q - R(t)$ is in $\mathcal{I}$. It implies that the reduction of Q and $R(t)$ with respect to ST are the same (we use here confluence property of standard basis). As the leading monomial is decreasing during the reduction process, the reduction of $R(t)$ is in $k[t]$, for any term implying x_i would be greater than the leading term of $R(t)$ with respect to $\prec$ (here is where we need an elimination ordering).

($\Leftarrow$) If R is the reduction of Q, $Q(x) - R(t)$ is in $\mathcal{I}$. But as $\mathcal{I}$ is the kernel of G, $Q(x) - R(P) = 0$. So Q is in $k[P]$ and R gives its expression in function of $P_1, \ldots, P_m$.

COROLLARY 1. *if f admits a polynomial inverse, then ST contains n polynomials of the form $x_i - R_i(t)$ for $i = 1, \ldots, n$, and the R_i defined an inverse of f.*

PROOF. We already know that we can can find in $\mathcal{I}$ n such polynomials. they must reduce to 0, with respect to ST. From the property of $\prec$, the leading term of any of them is of the form x_i. So we can find in ST a polynomial whose leading term is x_i for any $i = 1, \ldots, n$. the standard basis ST is reduced, hence they have to be of the wanted form.

The last part is a simple consequence of the proposition.

The last corollary gives us a way of testing inversibility and getting the expression of an inverse.

COROLLARY 2. *In the special case $n = m$, inversibility means that f is in fact one to one. Calling F the restriction of G to $k[t]$, F is also one to one and the polynomial R_i define its inverse. Furthermore ST is equal to $\{x_i - R_i(t)\}$*

PROOF. the two first parts are known and simple results (see [B]). the second implies that $\mathcal{I} \cap k[t]$ is (0), so the leading terms of any polynomial in ST must depend only of x_i for some i. As ST is reduced, it is therefore of the stated form.

As this situation is related to the well known jacobian conjecture, many other "tests" have been proposed for it (see [B]). Many of them have a mere theoretical interest. K. ADJAMAGBO has recently proposed a differential test, relying on the same result of GABBER we are going to use in the next section (see [A]).

REMARK 1. (About orderings) the lexicographic ordering on $x_1, \ldots, x_n, t_1, \ldots, t_m$ has obviously the wanted property

Nevertheless, it is certainly not the most efficient. the elimination ordering of D. BAYER and M. STILLMAN, used in their standard basis system MACAULAY would be a very better choice. Unfortunately, it does not seem to be available in any existing computer algebra system.

1.2. Inversibility in Rational Case

Let us come now to to the case where

$$\begin{array}{llll} f: & k^n & \longrightarrow & k^m \\ & (x_1, \ldots, x_n) & \longrightarrow & \left(\frac{P_1(x_1,\ldots,x_n)}{Q_1(x_1,\ldots,x_n)}, \ldots, \frac{P_m(x_1,\ldots,x_n)}{Q_m(x_1,\ldots,x_n)}\right) \end{array}$$

is a rational map. We state a general result, which is a slight extension of a theorem that SHANNON and SWEEDLER gave in the birational case and for f polynomial (see [SS1]). Again, we give ourselves m tag variables t_i and m more "inverse" variables u_i and consider the ideal I of $k[u_1, \ldots, u_m, x_1, \ldots, x_n, t_1, \ldots, t_m]$, generated by the m polynomials $P_i - Q_i t_i$ and the m other $Q_i u_i - 1$.

PROPOSITION 1. *the ideal $\mathcal{I}$ is prime.*

PROOF. Consider the ring homomorphism

$$\begin{array}{llll} G: & k[u, x, t] & \longrightarrow & k(x) \\ & x_i & \longrightarrow & x_i \\ & u_j & \longrightarrow & Q_j^{-1} \\ & t_k & \longrightarrow & P_k Q_i^{-1}. \end{array}$$

We claim that $\mathcal{I}$ is the kernel of G, which imply the proposition (see [SS2] for a more detailed proof).

DEFINITION 2. A admissible ordering $\prec$ on monomials of $k[u, x, t]$ is said to *eliminate globally* $u_1, \ldots, u_m$ *and successively* $x_1, \ldots, x_n$ if for any two monomials $m_1 = u^\alpha x^\beta t^\gamma$ and $m_2 = u^\delta x^\varepsilon t^\zeta$,

$$\begin{array}{rll} & \sum_{i=1}^m \alpha_i < \sum_{i=1}^m \delta_i & \\ \text{or} & \sum_{i=1}^m \alpha_i = \sum_{i=1}^m \delta_i & \Rightarrow \quad m_1 \prec m_2. \\ \text{and} & \exists\ 1 \le i \le n\ \beta_j = \varepsilon_j \text{ for } j < i \text{ and } \beta_i < \varepsilon_i & \end{array}$$

PROPOSITION 2. *In the situation given above, let $\mathcal{I}'$ be the intersection of $\mathcal{I}$ and $k[x,t]$. then taking the reduced standard basis ST of $\mathcal{I}$ for any admissible ordering $\prec$ which eliminates globally the $u_1,\ldots,u_m$ the polynomials in ST whose leading terms only depend of $x_1,\ldots,x_n,t_1,\ldots,t_m$ form a standard basis of $\mathcal{I}'$, and a fraction $R=\frac{M}{N}$ is in $k(\frac{P}{Q})$ iff there exist a reduced fraction $\frac{A}{B}$ of $k(t)$ such that B does not belong to $\mathcal{I}'$, and $MB-AN$ is in $\mathcal{I}'$.*

PROOF. The first part is an easy result, using the property of $\prec$.

($\Rightarrow$) We first prove the following lemma.

LEMMA 1. *Let $\mathcal{J}$ be any ideal over a k-algebra A, and $P_iQ_i'-P_i'Q_i$ be r members of $\mathcal{J}$. take any fraction R of $k(z_1,\ldots,z_r)$ and associate to it*

$$S=R(\frac{p_i}{q_i})=\frac{M(p,q)}{N(p,q)}\in k(p_1,\ldots,p_r,q_1,\ldots,q_r).$$

then $M(P_i,Q_i)N(P_i',Q_i')-M(P_i',Q_i')N(P_i,Q_i)$ belongs to $\mathcal{J}$.

PROOF. Call $\omega(R)$ the member of $\mathcal{J}$ we associate to R. We only have to prove that for all R and R' in $k(z_1,\ldots,z_r)$

$$\begin{array}{lcl} \omega(R)\in\mathcal{J} & \Rightarrow & \omega(R^{-1})\in\mathcal{J}\\ \omega(R)\in\mathcal{J}\text{ and }\omega(R')\in\mathcal{J} & \Rightarrow & \omega(R+R')\in\mathcal{J}\\ \omega(R)\in\mathcal{J}\text{ and }\omega(R')\in\mathcal{J} & \Rightarrow & \omega(RR')\in\mathcal{J}, \end{array}$$

which can be verified by simple calculations.

If R is in $k(\frac{P}{Q})$, let $\frac{A}{B}$ be a reduced fraction such that $\frac{A(\frac{P}{Q})}{B(\frac{P}{Q})}$ equals R. Let $\frac{C(p,q)}{D(p,q)}=A(\frac{p}{q})$ in $k(p,q)$. From the lemma, we know that $C(P,Q)D(t,1)-C(t,1)D(P,Q)=S(x)(MB-AN)$ is in $\mathcal{I}$. Hence $MB-AN$ is in $\mathcal{I}'$ for $\mathcal{I}'$ is prime.

($\Leftarrow$) Now, if $MB-AN$ is in $\mathcal{I}'$, and B is not, we just have to use the fact that $\mathcal{I}'$ is the kernel of G to conclude.

Sadly, we cannot use this to get the expression of R in $k(\frac{P}{Q})$, or even solve the membership problem except if $k(\frac{P}{Q})$ is $k(x_1,\ldots,x_n)$, which is the aim of the next theorem. We will see in part 2.2. how to solve the membership problem with another method. The reader can refer to [SS2] to see how that technique can be used to solve the membership problem for $k[\frac{P}{Q}]$.

THEOREME 1. *If f is defined as above and if ST is the standard basis of $\mathcal{I}$ for an ordering which eliminates globally $t_1,\ldots,t_m$ and successively $x_1,\ldots,x_n$, the two following properties are equivalent:*

(1) f admits an inverse,

(2) for each $i=1,\ldots,n$ there exits in ST a polynomial of the form $B_i(t)x_i-A_i(t)$.

then the fractions $\frac{A_i}{B_i}$ give the expression of an inverse.

PROOF. ($\Rightarrow$) It suffices to apply the last proposition, to know that such polynomials are in $\mathcal{I}'$ As the ordering eliminates successively $x_1,\ldots,x_n$, they must be in ST.

($\Leftarrow$) Now, if such polynomials are in ST, A_i is not in $\mathcal{I}$ for ST is reduced. We conclude as in prop. 1.

COROLLARY 1. *If $n=m$, let $\mathcal{J}$ be the ideal of $k(t)[u,x]$ generated by the same polynomials as above, and ST the reduced standard basis of $\mathcal{I}$ for an ordering which eliminates globally the u_i. then the two following properties are equivalent:*

(i) f is birational,

(ii) ST contains n polynomial of the form $x_i-M_i(t)$.

the inverse is defineded by the n fractions M_i.

PROOF. We only have to remark that if f is birational, $\mathcal{I}\cap k[t]$ is $\{0\}$ and then use the theorem.

REMARK 1. (About orderings) Another time, the lexicographic ordering satisfies the wanted property

... But to use it would be a disaster. Elimination is very expensive, so it is essential to use it as few as possible. unfortunately, no computer algebra system allow a better choice.

REMARK 2. (About inverse variables) If Q_i belongs to k one can obviously forget all about u_i. As pointed out in [SS], we can only use one inverse variable u and replace $u_iQ_i - 1$ by $uQ_1 \dots Q_m - 1$. We can also use more variables and lower the degree by taking all the factors of the Q_i. We think it is better in most cases to keep the maximum degree of the generating polynomial small, even if that increases the number of variables.

1.3. A Bound for Birational Mappings

We have given so far necessary and sufficient condition for inversibility, without caring much for complexity. But we know by experience that such calculations are much faster in the inversible case. So we need a bound to avoid unusefull calculations in "bad" cases. It is done by using a theorem, proved by O. GABBER, valid in birational case. So, until the end of this part, f will denote a rational map from k^n to k^n.

PROPOSITION 1. *There is a one to one correspondence between rational maps (resp. birational maps) from k^n to k^n and rational (resp. birational) maps from P_n to P_n.*

PROOF. See [H].

DEFINITION 3. Let F be a rational map from P_n to P_n, defined by

$$F(x_0, \dots, x_n) = (R_0, \dots, R_n),$$

where the R_i are n homogeneous polynomials without common factor. We call *degree* of F the common degree of the R_i. If f is a rational map from k^n to k^n, the degree of f is the degree of the corresponding homogeneous map.

PROPOSITION 2. *If f is polynomial, its degree if the maximum degree of the P_i. In the general case, the degree of f is bounded by the maximum degree of the P_i and of the product of the Q_i.*

PROPOSITION 3. (GABBER) *If f is birational, then*

$$\deg f^{-1} \leq (\deg f)^{n-1}.$$

PROOF. See [B].

THEOREME 1. *If f is a polynomial map of degree d, admitting a birational inverse, polynomials of th. 1.2.1 appears in the standard basis of $\mathcal{I}$ where calculations are truncated in degree less than $d^n + 1$.*

PROOF. We first remark that in the polynomial case, we can forget the inverse variables and consider $\mathcal{I}$ to be the ideal of $k[x,t]$ generated by $P_x - t_i$. We define then a weight function p on variables $x_1, \dots, x_n, t_1, \dots, t_n$, such that $p(x_i) = 1$ and $p(t_i) = \deg P_i$. So we have a graduation $\deg_p$ on monomials of $k[x,t]$, such that $\deg_p(x^\alpha t^\beta) = \sum_{i=1}^n \alpha_i + \sum_{i=1}^n \beta_i p(t_i)$.

We take then another variable x_0 of weight 1, and we homogenize $\mathcal{I}$ for graduation $\deg_p$ with respect to x_0. We write $\widetilde{S}$ the polynomial S homogenized, $\widetilde{\mathcal{I}}$ the ideal $\mathcal{I}$ homogenized. $\widetilde{\mathcal{I}}$ is equal to $(\widetilde{P_i} - t_i$ in $k[x_1, \dots, x_n, t_1, \dots, t_n, x_0]$. $\widetilde{\mathcal{I}}$ is prime for it is the kernel of:

$$\begin{array}{lcl} k[x_1, \dots, x_n, t_1, \dots, t_n, x_0] & \xrightarrow{\phi} & k[x_0, x_1, \dots, x_n] \\ x_i & \longrightarrow & x_i \\ t_i & \longrightarrow & \widetilde{P}_i(x). \end{array}$$

We further remark that we can extend any admissible ordering $\prec$ on monomials of $k[t_1, \dots, t_n]$ to an admissible ordering $\widetilde{\preceq}$ on monomials of $k[x_1, \dots, x_n, t_1, \dots, t_n, x_0]$ of the same degree by evaluating x_0 to 1 and then applying $\prec$. So there is a one to one correspondence between standard basis calculations for any ideal $\mathcal{J}$ generated by $S_1, \dots, S_p$ in $k[x_1, \dots, x_n, t_1, \dots, t_n]$ with respect to $\prec$, and standard basis calculations for $\widetilde{\mathcal{J}}$, if it is generated by $\widetilde{S}_1, \dots, \widetilde{S}_p$ in $k[x_1, \dots, x_n, t_1, \dots, t_n, x_0]$, with respect to $\widetilde{\preceq}$.

As $\widetilde{I}$ must contain a polynomial of the form $(\widetilde{Q_i x_i - Q_i}) x_0^k$ (using th. 2.1.) and $x_0 \notin \widetilde{\mathcal{I}}$, we deduce that $\widetilde{\mathcal{I}}$ contains $(\widetilde{Q_i x_i - R_i})$ whose degree $\deg_p$ is less than $(\deg f)^n + 1$. Indeed we have two cases

$$\begin{array}{rcl} \deg_p(\widetilde{Q_i x_i - R_i}) = \deg_p \widetilde{R}_i & \leq & max_i\{p(Y_i)\} \deg R_i \\ & \leq & \deg f \ \deg R_i \end{array}$$

or

$$\deg_p(\widetilde{Q_i x_i - R_i}) = \deg_p \widetilde{Q}_i x_i \begin{array}{l} \leq \ max_i\{p(Y_i)\} \ \deg Q_i + 1 \\ \leq \ \deg f \ \deg R_i + 1. \end{array}$$

Then we only have to use the result of GABBER to show it is less or equal to $d^n + 1$.

$\widetilde{\mathcal{I}}$ being homogeneous with respect to $\deg_p$, we can truncate the standard basis in degree $\deg_p \leq (\deg f)^n$. But as the ordinary degree is less or equal to $\deg_p$, we can a fortiori truncate it in degree $(\deg f)^n$.

Then, we evaluate x_0 à 1, which cannot increase the degree and get the wanted result.

REMARK 1. We think a bound of the form $\varepsilon d^{\alpha n}$ could be obtained for f rational. It should be only a technical problem to free the proof of the homogeneity argument.

2. Standard Basis and Symmetrical Variables

2.1. Membership Problem and Inversibility in Rational Case

We return to the general case with another method. Instead of using m tag variables taking the place of P_i/Q^i, we take n "symmetrical" variables y_i taking the place of x_i. We associate to f the ideal $\mathcal{J}$ of $k(y_1, \ldots, y_n)[u_1, \ldots, u_m, x_1, \ldots, x_n]$ generated by the $2m$ polynomials $Q_i(x)u_i - 1$, and $P_i(x) - \frac{P_i(y)}{Q_i(y)} Q_i(x)$. We define the morphism:

$$\begin{array}{rlcl} \phi: & k[u, x, t] & \longrightarrow & k(y)[u, x] \\ & x_i & \longrightarrow & x_i \\ & u_j & \longrightarrow & u_j \\ & t_k & \longrightarrow & \frac{P_k(y)}{Q_i(y)}. \end{array}$$

THEOREME 1. *The fraction $S = M/N$ belongs to $k(P/Q)$ iff the polynomial $M(x) - M(y)N^{-1}(y)N(x)$ belongs to $\mathcal{J}$.*

PROOF. ($\Rightarrow$) It is obvious that $\phi(\mathcal{I})$ is included in $\mathcal{J}$. We apply this to the polynomial of prop. 1.2.2.

($\Leftarrow$) As the polynomials defining $\mathcal{J}$ are in $k(P(y)/Q(y))[u, x]$ we can consider the ideal $\mathcal{J}'$ they generate in this ring. The wanted polynomial is in $\mathcal{J}'$ by the same argument as above, so $M(y)/N(y)$ belongs to $k(P(y)/Q(y))$.

We now have an algorithm to solve the membership problem. All we have to do is calculate the standard basis of $\mathcal{J}$ with respect to *any* ordering, and reduce $M(x) - M(y)/N(y)N(x)$.

COROLLARY 1. *Let ST be the reduced standard basis of $\mathcal{J}$, for an ordering which eliminates globally $u_1, \ldots, u_m$, the two following propositions are equivalent:*

(i) f admits an inverse,

(ii) $ST = \{x_i - y_i, u_j - Q_j^{-1}(y)\}$.

PROOF. We know that f admits an inverse iff $k(P/Q)$ is equal to $k(x)$. So by the last theorem $x_i - y_i$ have to be in $\mathcal{J}$. Then the property of the ordering imply they are in ST. Reducing $u_i Q_i(x)$ with respect to these n polynomials, we find that $u_i - Q_i(y)$ is in $\mathcal{J}$ and so in ST.

PROPOSITION 1. *The bound of th. 1.3.1. is still valid in this case.*

REMARK 1. If f is polynomial we can obviously forget the u_i.

2.2. the Polynomial Case

f is now a polynomial map from k^n to k^n, defined by n polynomials P_i. We associate to it a ideal $\mathcal{I}$ of $k[x_1, \ldots, x_n, y_1, \ldots, y_n]$, generated by the n polynomials $P_i(x) - P_i(y)$.

PROPOSITION 1. *Let ST be the reduced standard basis of $\mathcal{I}$ for any ordering $\prec$ with $x_i \prec y_j$, then f admits a polynomial inverse iff ST equals $\{x_i - y_i\}$ and the standard basis calculation can be truncated in degree d^n.*

PROOF. ($\Rightarrow$) If f admits a polynomial inverse, defined by n polynomials Q_i, $Q_i(f(x)) - Q_i(f(y))$ belongs to $\mathcal{I}$ and is equal to $x_i - y_i$. It suffices now to use the property of the ordering to see that those n polynomials form the standard basis. ($\Leftarrow$) We can suppose k is algebraicaly closed by replacing it by its algebraic closure.

It is known then (see [B]) that if f is an univalent it admits a polynomial inverse. Now, if $x_i - y_i$ is in $\mathcal{I}$ for all i, f is univalent.

The proposition does not extend in the situation where f is from k^n to k^m with $m > n$.

EXAMPLE 1. If we take $f(x_1, x_2) = (x_1, x_1x_2, x_1x_2^2 + x_2)$, it is easy to check that $\mathcal{I}$ is equal to $\{x_1 - y_1, x_2 - y_2\}$ which means that f is univalent, but $k[x_1, x_1x_2, x_1x_2^2 + x_2]$ is different from $k[x_1, x_2]$. So f admits no polynomial inverse.

2.3. A Bound for De JONQUIÈRE's Maps

We will show that some assumption on the form of f, a polynomial map defined by $P_1, \ldots, P_m$, allow us to majorate the degree in the standard basis calculation with a better bound. It has been conjectured by SEGRE that if f is a polynomial map from k^n to k^n admitting a polynomial inverse, it can be obtained as a composition of one to one linear maps and maps of DE JONQUIÈRE, of the form: $g(x_1, \ldots, x_n) = (\rho_1(x_1, \ldots, x_n), \ldots, \rho_n(x_1, \ldots, x_n))$, where

$$\begin{aligned}
\rho_1 &= x_1 \\
\rho_2 &= x_2 + P_2(x_1) \\
&\vdots \\
\rho_n &= x_n + P_n(x_1, \ldots, x_{n-1}).
\end{aligned}$$

We suppose f is a polynomial map that can be obtained as a composition of one to one linear maps and maps of the form $g(x_1, \ldots, x_r) = (\rho_1(x_1, \ldots, x_n), \ldots, \rho_s(x_1, \ldots, x_n))$ where $s > r$ and

$$\begin{aligned}
\rho_1 &= x_1 \\
\rho_2 &= Q_2(x_1)\theta_2 + P_2(x_1) \\
&\vdots \\
\rho_r &= Q_n(x_1, \ldots, x_{r-1})x_n + P_n(x_1, \ldots, x_{n-1}). \\
\rho_{r+1} &= P_{r+1}(x_1, \ldots, x_r) \\
&\vdots \\
\rho_s &= P_s(x_1, \ldots, x_r).
\end{aligned}$$

If $f = \rho_1 \circ \ldots \circ \rho_h$, we suppose further that:

$$\forall 1 \leq i < r \ \deg(\rho_1 \circ \ldots \rho_i) \leq \deg(\rho_1 \circ \ldots \rho_i).$$

DEFINITION 4. If a map f satisfy our assumption, it is said to admit an *extended Segre form*.

DEFINITION 5. Let $A = \{Q_1, \ldots, Q_k\}$ be a finite set of polynomials of $k[x_1, \ldots, x_n]$, an admissible ordering been given any of them can be considered as a rewrite rule $\xrightarrow{Q_i}$. Then we call a *chain of reduction from* A, a finite list of polynomials $T_1, \ldots, T_r$ such that T_i is equal to Q_i for $i = 1 \ldots, n$ and for each $i = n+1, \ldots, r$ there exist $j, j' < i$ such that

$$T_j \xrightarrow{T_{j'}} T_i \ \text{ or } \ T_j \xleftarrow{T_{j'}} T_i.$$

The *degree* of the chain is the maximum degree of the T_i.

PROPOSITION 1. *If f of degree d admits an extended Segre form, then it admits a rational inverse and the standard basis of the ideal $\mathcal{I}$ of $k(y)[x]$ generated by the n polynomials $P_i(x) - P_i(y)$ is $\{x_i - y_i\}$ can be calculated in degree less or equal to d.*

PROOF. f obviously admits a rational inverse, for each ρ_i does. Now, we know than the standard basis is of the wanted form from cor 1. of th. 2.1. To prove it can be obtained by a standard basis calculation in degree less than $\deg f$, we use the following two lemmas.

Lemma 1. *We call $\mu_{i,j}$ the m_i polynomials defining $\rho_1 \circ \ldots \circ \rho_i$ and define $\mu_{0,i}$ as x_i. Then for all $i < h$ and all $j = 1, \ldots, m_{i-1}$, $\mu_{i-1,j}(x) - \mu_{i-1,j}(y)$ appear in a chain of reductions of degree d from $\{\mu_{i,j}(x) - \mu_{i,j}(y)\}$.*

This imply that $x_i - y_i$ appear in a chain of reductions of degree d from $\{P_i(x) - P_i(y)\}$. We use then the second lemma.

Lemma 2. *If the polynomial R appears in a chain of reductions of degree d from $\{Q_1, \ldots, Q_k\}$, R is reduced to 0 by the set of polynomials calculated during a standard basis calculation truncated in degree d.*

The second lemma imply that $x_i - y_i$ appear during the standard basis calculation truncated in degree d.

3. Application to Global Indentifiability and Other Problems

3.1. Some Automatics

We will be interested in linear state space structures with zero initial conditions. Such a structure M is a set of models $M(\theta)$ defined by:

$$\begin{array}{lcl} dx/dt & = & A(\theta)x + B(\theta)u(t) \\ y & = & C(\theta)x \\ x(0) & = & 0, \end{array}$$

where the input function $u(t) \in u$ denotes the action of the experimentator (u is generaly the set of piecewise-continuous functions), the state vector $x \in \mathbf{R}^q$ denotes the internal state of the physical or chemical system described by the model, the output vector $y \in R^r$ denotes the values measured during the experiment, and $\theta \in D \subset \mathbf{R}^n$ denotes internal parameters of the system.

We will now state some formal definitions.

Definition 6. A property is said to be *structural* if it is valid for almost all models of a structure.

Definition 7. A model $M(\theta)$ is *globally identifiable* if for all θ'

$$y(t, \theta', u) = y(t, \theta, u) \Rightarrow \theta' = \theta.$$

Definition 8. According to the preceding definitions, a structure M is said to be *globally identifiable* if almost all model $M(\theta); \theta \in D$ is.

In practice this means that we want to know a priori if we have a probability 1 to determine a unique value of θ and a unique model, from the experimental results. Such definitions could be given for structures described by other kinds of differential system. But the considered case has the nice property that we can summarize its input-output behaviour with a polynomial function of the coefficient of A, B and C, by taking the coefficients of the transfer matrix, or the Markov parameters. We suppose for now on that the coefficients of A, B and C are polynomials in θ. So we only have to test the structural univalence of a polynomial map $f(\theta)$. The reader can refer to [L], [R] or [LW] for more details.

So the problem is now to test whether there exist a subset E of D such that f restricted to $D \setminus E$ is an one to one. In practice the answer can often been given by considering only the complex case.

Proposition 1. *Let f from $\mathbf{C}^n$ to$\mathbf{C}^m$ be a polynomial map. then, there exist a domain E of zero measure such that f restricted to $C^n \setminus E$ is an one to one iff f admits a rational inverse.*

This property allow us to use cor 1. of th. 2. 1. where we can forget the u_i for f is polynomial. If f admits no inverse, we can use the standard basis calculated to get more precise information. For example, if the set of solution is of dimension greater than zero, we know that f is not structuraly one to one even in real case.

3.2. An Implementation in Scratchpad II

The implementation we made in SCRATCHPAD II contains two main parts. The first is the domain STRUCTLS, whose elements represent linear structures with zero initial conditions. They are mostly represented as a record of three matrix. It allows the calculation of classical summaries as Markov parameters or coefficients of the transfer matrix. Other "special" summaries could be calculated with existing functions of SCRATCHPAD II. We have developed many functions to store information about the structure in ordering not to repeat calculations. Structures can also easily be stored on disk, for further use.

The package IDPACK realize the test of inversibility. It builds the list of polynomials $P_i(x) - P_i(y)$ and then calls the standard basis package of SCRATCHPAD II. It answers `True` if the standard basis has the form of cor. 1. of th. 2.1.1. and `False` in all other cases. Of course, in this case we cannot be sure of it, except if the dimension of the ideal is greater than zero. In general, the user can recover the result of the standard basis calculations which has been stored. As we use degree ordering, we cannnot solve the system yet. But, the package implemented by J.C. Faugère in SCRATCHPAD (see [FGLM]) allow us to get easily the standard basis for lexicographic ordering. In this form, we can try to define extra solutions and check if they can or not be in D. This part of work has not yet been developed in our implementation.

Another function treat the case where f is rational, which we do not need yet for structural identifiability. We will see an application for it with the last example.

3.3. Examples

Example 1. ([L] p. 105) In this example, we consider the following structure:

$$\begin{array}{rcl} \frac{dt}{dx} & = & \begin{array}{cccc} -(\theta_1+\theta_2) & 0 & 0 \\ \theta_1 & -\theta_3 & 0 \\ \theta_2 & \theta_3 & -\theta_4 \end{array} x + \begin{array}{c} 1 \\ 0 \\ 0 \end{array} u \\ y & = & \begin{array}{ccc} 0 & \theta_6 & 0 \\ 0 & 0 & \theta_7. \end{array} \end{array}$$

Calculating the transfer matrix, we find the summary defined by polynomials:

$$\begin{array}{rcl} \rho_1 & = & \theta_1\theta_6 \\ \rho_2 & = & \theta_1\theta_6 \\ \rho_3 & = & \theta_2\theta_7 \\ \rho_4 & = & \theta_7\theta_3(\theta_1+\theta_2) \\ \rho_6 & = & \theta_1+\theta_2+\theta_3 \\ \rho_7 & = & \theta_3(\theta_1+\theta_2) \\ \rho_8 & = & \theta_3(\theta_1+\theta_2)+\theta_4(\theta_1+\theta_2+\theta_3) \\ \rho_9 & = & \theta_4\theta_3(\theta_1+\theta_2.) \end{array}$$

Computing the standard basis of $\mathcal{I}$ in $k(\theta')[\theta]$, we get two solutions: $\theta\ = \theta'$ and

$$\begin{array}{rcl} \theta_1 & = & \theta'_3-\theta'_2 \\ \theta_2 & = & \theta'_2 \\ \theta_3 & = & \theta'_1+\theta'_2 \\ \theta_4 & = & \theta'_4 \\ \theta_6 & = & \theta'_1\theta'_6/(\theta'_3-\theta'_2) \\ \theta_7 & = & \theta'_7. \end{array}$$

It can be shown, using lemma 2. of th. 2.3.1. that the standard basis can be calculated in degree 3, which is the maximum degree of the ρ_i.

Example 2. ([R] p. 115) In this example, ordinary summaries would be too great to be computed. But the knowledge of the system allow us to find a smaller one, which have been computed in SCRATCHPAD II. Then we discovered Raksanyi made a mistake, and that the structure is not identifiable, as it is said in

[R]. Applying his method with the right summary, his program stopped by lack of memory after many hours of calculations. It only takes only 156.467 s to get the standard basis in SCRATCHPAD II.

EXAMPLE 3. The last example has no connection with identifiability. We want to test whether f from $\mathbf{C}^9$ to $\mathbf{C}^{12}$ defined by the 12 polynomials $\rho_{i,j,k}; i,j,k = 1,2,3 j \neq ik \neq i$ in the 9 variables $s_{l,m}; l,m = 1,2,3$:

$$\rho_{i,j,k} = s_{j,k} + \frac{s_{j,i}s_{i,k}}{g_i - s_{i,i}}$$

admits a rational inverse. We give a part of the scratchpad session, where `lp` is the list of polynomials defining $\mathcal{I}$.

```
groebner lp
   loading GB LISPLIB K1 for package GroebnerPackage
   loading GBINTERN LISPLIB K1 for package GroebnerInternalPackage

   (10)
   [s11 - S11, s12 - S12, s13 - S13, s21 - S21, s22 - S22, s23 - S23, s31 - S31,

                                     1                  1                   1
    s32 - S32, s33 - S33, u1 + ----------, u2 + ----------,  u3 + ----------]
                               S11 - G1           S22 - G2            S33 - G3


   Type:
 L NDMP([s11,s12,s13,s21,s22,s23,s31,s32,s33,u1,u2,u3],QF
P[S11,S12,S13,S21,S22,S23,S31,S32,S33,G1,G2,G3]I)
   1.907 (IN) + 34.772 (EV) + 1.614 (OT) + 5.218 (GC) = 43.512 sec
```

We have simulated the tag variable method of th. 1.2.1. with MACAULAY by trying to eliminate globaly the u_i. We used MACAULAY because it is much more powerfull for standard basis, than the package of SCRATCHPAD even in a small computer SPS7 BULL. It stops by lack of memory after about a day of calculations.

References

[A] K. ADJAMAGBO and A. VAN DEN ESSEN *A Differential Criterion and Formula for the Inversion of a Polynomial Map in Several Variables* (to appear).

[B] H. BASS et al. *The jacobian conjecture: reduction of degree and formal expansion of the inverse*, Bulletin of the A.M.S. 7,2 , 1982.

[FGLM] J.C. FAUGÈRE, P. GIANNI, D. LAZARD and T. MORA *Efficient computation of zero-dimentional Gröbner bases by change of ordering*, 1988, preprint.

[H] Robin HARTSHORNE, *Algebraic Geometry*, Graduate Texts in Mathematics ; 52, Springer Verlag, 1977.

[L] Yves LECOURTIER *Propriétés structurelles de modèles, Etudes théoriques, tests formels, Applications à la catalyse hétérogène*, thèse de Doctorat ès Sciences, université Paris-Sud, 1985.

[LW] Yves LECOURTIER and Eric WALTER, *The testing of STructural Properties throught Symbolic Computation* in *Identifiability of Parametric models*, ch. 7., ed. E. Walter, Pergamon, Oxford, 1987.

[O1] François OLLIVIER *Le problème de l'identifiabilité structurelle globale en automatique*, preprint to appear in CALSYF VIII ,1988.

[O2] François OLLIVIER *Une borne sur le degré des calculs intermédiaires pour déterminer l'inverse d'une application birationnelle par l'algorithme de base standard*, preprint ,1988.

[R] Atilla RAKSANYI *Utilisation du calcul formel pour l'étude des systèmes d'équations polynomiales (application en modélisation)*, thèse de Doctorat ès Sciences, université Paris-Dauphine, 1986.

[RLWV] Atilla Raksanyi, Yves Lecourtier, Eric Walter and Allain Venot *Identifiability and Distinguishability testing Via Computer Algebra*, Mathematical Biosciences, 77, 245–266, 1985.

[SS1] David Shannon and Moss Sweedler *Using Groebner bases to determine algebra membership, split surjective algebra homomorphisms and determine birational equivalence*, preprint, 1987.

[SS2] David Shannon and Moss Sweedler *Using Groebner bases to determine subalgebra membership*, preprint, 1988.