A RESULTANT CRITERION AND FORMULA FOR THE INVERSION OF A POLYNOMIAL MAP IN TWO VARIABLES

Kossivi ADJAMAGBO
Département de Mathématiques, Université de Paris VI, 75252 Paris, France

Arno van den ESSEN
Mathematisch Instituut, Faculteit der Wiskunde en Natuurwetenschappen, Katholieke Universiteit, Toernooiveld, 6525 ED Nijmegen, Netherlands

Communicated by J. Rhodes
Received 17 January 1989

A criterion is given for the invertibility of a polynomial map in two variables over an arbitrary field. A formula for the inverse is derived as well as other results obtained by McKay and Wang.

Introduction

Let \( k \) be an arbitrary field and \( F : k^n \to k^n \) a polynomial map \( (n \geq 1) \) i.e. \( F \) is given by coordinate functions \( F_i \) which are polynomials in \( n \) variables \( X_1, \ldots, X_n \) over \( k \). The question: ‘How can one recognize when such an \( F \) is invertible (with an inverse which is also a polynomial map)?’, has attracted the attention of many authors. In particular, if the characteristic of \( k \) is zero, the conjecture that \( F \) is invertible if and only if the determinant of the Jacobian matrix is a non-zero constant (the Jacobian conjecture), has been studied by many people, but remains still an unsolved problem (if \( n \geq 2 \)). For more details about this conjecture we refer the reader to [2].

In [5] and [1] new criteria are given to decide if a polynomial map is invertible. In the second paper also a formula for the inverse is obtained.

In this paper we consider the case \( n = 2 \) and give another (simple) criterion for the invertibility of a polynomial map (Theorem 1.1). As an immediate consequence we derive a formula for the inverse, a result also obtained in [3], and show that \( F \) is completely determined by its border polynomials \( F_i(0,X_2) \) and \( F_j(X_1,0) \) (see also [3]).

At the end of this paper we formulate a conjecture (in case \( \text{char } k = 0 \)) and apply our main theorem to show that this conjecture is equivalent with the Jacobian conjecture.
0. Properties of the resultant of two polynomials in one variable

0.1. In this section $A$ denotes a commutative ring without zero divisors, $K$ its quotient field and $A[T]$ the polynomial ring in the variable $T$ with coefficients in $A$.

Let $f=f_nT^n+f_{n-1}T^{n-1}+\cdots+f_0$ be a polynomial in $A[T]$ with $f_n$ non-zero. Then the integer $n$ is called the degree of $f$, denoted $\deg f$, and the element $f_n$ is called the leading coefficient of $f$, denoted $\text{lc}_T f$. Let $g=g_mT^m+g_{m-1}T^{m-1}+\cdots+g_0$ also be in $A[T]$ with $g_m$ non-zero.

(i) If $m,n\geq 1$, the resultant of $f$ and $g$, denoted $R_T(f,g)$ is defined as

$$R_T(f,g) = \det \begin{pmatrix} f_n & \cdots & f_0 \\ \vdots & \ddots & \vdots \\ f_n & \cdots & f_0 \\ g_m & \cdots & g_0 \\ \vdots & \ddots & \vdots \\ g_m & \cdots & g_0 \end{pmatrix}.$$ 

(ii) If $m=0$ we put $R_T(f,g)=g_0^n$ and if $n=0$ we put $R_T(f,g)=f_0^m$.

From (i) we observe that the diagonal of the matrix above consists of the elements $f_n$ ($m$ times) and $g_0$ ($n$ times), which gives the contribution $f_n^m g_0^n$ to the resultant. Since $R_T(f,g)=(-1)^{mn} R_T(g,f)$ (interchange the rows) we also find the contribution $(-1)^{mn} g_m^m f_0^m$ to the resultant $R_T(f,g)$. In case (ii) both terms are equal and contribute to the resultant. Summing up we get

The resultant $R_T(f,g)$ contains the terms $f_n^m g_0^n$ and $(-1)^{mn} g_m^m f_0^m$. (0.2)

Furthermore, the resultant has the following properties (see [4, $\S$43]):

$f$ and $g$ have a zero in common (in some field extension of $K$) if and only if $R_T(f,g)=0$ (0.3)

There exist polynomials $a$ and $b$ in $A[T]$ such that $R_T(f,g)=af+bg$. (0.4)

0.5. For the applications in Section 1 we need to introduce two more variables $Y_1$ and $Y_2$ and form $f - Y_1$ and $g - Y_2$, which we consider as polynomials in $T$ with coefficients in the ring $A[Y]:=A[Y_1,Y_2]$. So by 0.1, $R_T(f - Y_1, g - Y_2)$ is a well-defined element in $A[Y]$, i.e. a polynomial in $Y_1$ and $Y_2$ with coefficients in $A$, which we denote by $R$. Observe that

$$\deg_Y R \leq \max(n,m)$$ (0.6)

(to see this one only needs to develop the determinant in 0.1(i), with $f_0$ replaced by $f_0 - Y_1$ and $g_0$ replaced by $g_0 - Y_2$, after the first $\min(n,m)$ columns. In case $n$ or $m$ are zero, the formula is obvious).

Furthermore, the definition of $R$ and (0.2) imply that

$$\deg_{Y_1} R = m, \quad \deg_{Y_2} R = n, \quad \text{lc}_{Y_1} R = (-1)^{m+mn} g_m^n, \quad \text{lc}_{Y_2} R = (-1)^n f_n^m.$$ (0.7)
1. Invertible polynomial maps and the main theorem

Let \( k \) be an arbitrary field and \( k[X, Y] := k[X_1, X_2, Y_1, Y_2] \) the polynomial ring in the variables \( X_1, X_2, Y_1, Y_2 \) over \( k \). Let \( F_1 \) and \( F_2 \) be two polynomials in the \( k \)-subalgebra \( k[X] := k[X_1, X_2] \). So they define a polynomial map \( F \) from \( k^2 \) to \( k^2 \) (by putting \( F(x_1, x_2) = (F_1(x_1, x_2), F_2(x_1, x_2)) \)). We call such a polynomial map invertible if there exist polynomials \( G_1 \) and \( G_2 \) in \( k[Y] \) such that \( F_i(G_1, G_2) = Y_i \) for all \( i = 1, 2 \).

By an argument, similar to the one given in the proof of Theorem 1.1, (ii) \( \Rightarrow \) (i) below, one easily deduces that \( G_i(F_1, F_2) = X_i \) for all \( i = 1, 2 \). So the polynomial map \( G \) defined by \( G_1 \) and \( G_2 \) is the inverse of \( F \) and vice versa.

The main result of this paper is

**Theorem 1.1.** Let \( F = (F_1, F_2) \) be a polynomial map. There is equivalence between
(i) \( F \) is invertible.
(ii) There exist \( \lambda_1 \) and \( \lambda_2 \) in \( k^* \) and \( G_1 \) and \( G_2 \) in \( k[Y] \) such that
\[
R_{X_i}(F_1 - Y_1, F_2 - Y_2) = \lambda_1(X_1 - G_1) \quad \text{and} \quad R_{X_i}(F_1 - Y_1, F_2 - Y_2) = \lambda_2(X_2 - G_2).
\]
Furthermore, if \( F \) is invertible, then \( G = (G_1, G_2) \) is the inverse of \( F \).

**Proof.** (ii) \( \Rightarrow \) (i) Consider the following ideal in \( k[X, Y] \): \( p = (X_1 - G_1, X_2 - G_2) \) and \( q = (Y_1 - F_1, Y_2 - F_2) \). By (ii) and (0.4) we get \( p \subseteq q \). Observe that \( k[X, Y]/q = k[X] \) and \( k[X, Y]/p = k[Y] \), so \( p \) and \( q \) are prime ideals of height two. Consequently \( p = q \).

So \( X_i - G_i \in q \), from which we deduce that \( X_i = G_i(F_1, F_2) \) (substitute \( Y_i = F_i \)). From \( Y_i - F_i \in p \) we deduce \( Y_i = F_i(G_1, G_2) \) (substitute \( X_i = G_i \)). So \( F \) is invertible with \( G \) as inverse, which proves (ii) \( \Rightarrow \) (i).

The last statement of the theorem follows from the implication (i) \( \Rightarrow \) (ii) and the previous arguments. So it remains to prove (i) \( \Rightarrow \) (ii).

**Lemma 1.2.** Put \( R_1 := R_{X_1}(F_1 - Y_1, F_2 - Y_2) \), \( R_2 := R_{X_2}(F_1 - Y_1, F_2 - Y_2) \). If \( F \) is invertible with inverse \( (G_1, G_2) \), then there exist polynomials \( \lambda_1 \) and \( \lambda_2 \) in \( k[X, Y] \) such that
\[
R_1 = \lambda_2(X_2 - G_2) \quad \text{and} \quad R_2 = \lambda_1(X_1 - G_1).
\]

**Proof.** The polynomials \( F_1(G_1, X_2) - Y_1 \) and \( F_2(G_1, X_2) - Y_2 \) considered as polynomials in \( X_2 \) with coefficients in \( k[Y] \) have \( G_2 \) as a common zero. Furthermore, \( \deg_{X_1} F_i(G_1, X_2) = \deg_{X_1} F_i(X_1, X_2) \), since for any non-zero polynomial \( a \) in \( k[X_1] \) also \( a(G_1) \) is non-zero (if \( a(G_1) = 0 \), then \( a(G_1(F_1, F_2)) = 0 \), i.e. \( a(X_1) = 0 \)). So by (0.3) their resultant with respect to \( X_2 \) is zero and \( R_2 \) considered as polynomial in \( X_1 \) with coefficients in \( k[Y] \) has a zero at \( X_1 = G_1 \). Hence \( X_1 - G_1 \) divides \( R_2 \) in \( k[Y][X_1] \) as desired. In a similar way we obtain the result for \( R_1 \).

**Corollary 1.3.** If \( F \) is invertible with inverse \( G \), then
Proof. Since $R_2 = \lambda_1(X_1 - G_1)$, $\deg_{Y_1} G_1 \leq \deg_{Y_1} R_2 \leq \deg F$ (by (0.6)). Similarly, using $R_1$ we obtain $\deg_{Y_1} G_1 \leq \deg F$. So $\deg G \leq \deg F$. Repeating the argument with $F$ and $G$ interchanged gives the opposite inequality, which concludes the proof. \(\square\)

Corollary 1.4. An invertible polynomial map $F$ has the following property:

(C) If $\deg_{X_i} F_i$ is positive, then $\text{lcm}_{X_i} F_i$ is a non-zero constant (all $i, j$).

Proof. Let $G$ be the inverse of $F$. It suffices to show that $G$ has property (C) (since $F$ is the inverse of $G$). So suppose $\deg_{Y_1} G_1$ is positive. Compare the leading coefficients, with respect to $Y_1$, in both sides of the equation $R_2 = \lambda_1(X_1 - G_1)$. Using (0.7) this gives

$$(-1)^{m_1 + m_2} (\text{lcm}_{X_i} F_i)^n = \text{lcm}_{Y_i} G_i. \quad (1.5)$$

Since the left-hand side is a non-zero polynomial in $k[X_1]$ and $\text{lcm}_{Y_i} G_i$ is a polynomial in $k[Y_1]$, it follows that $\text{lcm}_{Y_i} G_i$ is in $k^*$. Arguing in the same way for the other $\text{lcm}_{Y_i} G_i$ we conclude that $G$ has property (C). \(\square\)

Proof of Theorem 1.1 (concluded). It remains to prove that $\lambda_1$ and $\lambda_2$ (Lemma 1.2) belong to $k^*$. We only show this for $\lambda_1$ ($\lambda_2$ is treated similarly). From $R_2 = \lambda_1(X_1 - G_1)$ and (0.7) we obtain

$$\deg_{X_i} F_i \leq \deg_{X_i} X_1 \leq \deg_{X_1} F_2 \quad \text{and} \quad \deg_{Y_2} G_1 \leq \deg_{Y_2} R_2 = \deg_{X_1} F_1. \quad (1.6)$$

Similarly, $R_1 = \lambda_2(X_2 - G_2)$ and (0.7) give

$$\deg_{X_i} F_i \leq \deg_{X_i} X_2 \leq \deg_{X_2} F_1 \quad \text{and} \quad \deg_{Y_2} G_2 \leq \deg_{Y_2} R_1 = \deg_{X_2} F_2. \quad (1.7)$$

Interchanging the roles of $F$ and $G$ in this arguments gives

$$\deg_{X_i} F_i \leq \deg_{Y_2} F_2 \leq \deg_{Y_1} G_1, \quad \deg_{X_i} F_i \leq \deg_{Y_1} G_1; \quad \deg_{X_i} F_2 \leq \deg_{Y_2} G_1, \quad \deg_{X_i} F_2 \leq \deg_{Y_2} G_1. \quad (1.8)$$

So from (1.6), (1.7) and (1.8) we obtain in particular

$$\deg_{Y_1} G_1 = \deg_{X_1} R_1 \quad \text{and} \quad \deg_{Y_2} G_2 = \deg_{X_2} F_2. \quad (1.9)$$

So (1.9) and the relation $R_2 = \lambda_1(X_1 - G_1)$ imply that $\deg_{Y_1} \lambda_1 = \deg_{Y_2} \lambda_1 = 0$, i.e. $\lambda_1 \in k[X_1]$. If $\deg_{X_1} F_2 = 0$, then $F_2 = F_2(X_1)$ so by 0.1(ii) $R_2 = (F_2 - Y_2)^m$ for some integer $m \geq 1$. Since $\lambda_1$ is a polynomial in $k[X_1]$ which divides the non-zero polynomial $R_2$ we conclude that $\lambda_1 \in k^*$.

Finally, if $\deg_{X_1} F_2$ is positive, then by (1.6) and (1.9) also $\deg_{Y_1} G_1$ is positive. So by Lemma 1.2 both $\text{lcm}_{X_i} F_2$ and $\text{lcm}_{Y_i} G_1$ are non-zero constants, hence by (1.5) $\text{lcm}_{X_i} F_2 \in k^*$. However, $\text{lcm}_{X_i} \lambda_1 = \lambda_1$, since $\lambda_1 \in k[X_1]$, which gives that $\lambda_1$ belongs to $k^*$, as desired. \(\square\)
2. Some consequences of Theorem 1.1 and a conjecture

Notations as in Lemma 1.2. Write $R_1(X_2; Y_1, Y_2)$ (respectively $R_2(X_1; Y_1, Y_2)$) instead of $R_1$ (respectively $R_2$). Then Theorem 1.1 gives that $R_2(0; Y_1, Y_2) = -\lambda_1 G_1$ and $R_2(1; F_1(0), F_2(0)) = \lambda_1$ (since $G_1(F_1(0), F_2(0)) = 0$). Arguing in a similar way for $R_1$ we obtain:

**Theorem 2.1 (Inversion formula).** If $F$ is invertible with inverse $G$, then

$$G = \left( -\frac{R_2(0; Y_1, Y_2)}{R_2(1; F_1(0), F_2(0))}, -\frac{R_1(0; Y_1, Y_2)}{R_1(1; F_1(0), F_2(0))} \right).$$

If we call the polynomials $F_i(0, X_2)$ and $F_i(X_1, 0)$ ($i = 1, 2$) the ‘border polynomials’ of $F$ (following [3]), then we have

**Corollary 2.2.** If $F$ is invertible, then it is completely determined by its border polynomials.

**Proof.** Let $G$ be the inverse of $F$. Since $F$ is the inverse of $G$ it suffices to prove that $G$ is determined by the border polynomials of $F$. From Theorem 1.1 (or Theorem 2.1) we deduce that it remains to show that $\lambda_1$ and $\lambda_2$ are determined by the border polynomials of $F$. We only show this for $\lambda_1$ ($\lambda_2$ is treated in a similar way). Therefore consider the relation

$$R_2(F_1(0, X_2) - Y_1, F_2(0, X_2) - Y_2) = -\lambda_1 G_1.$$  \hspace{1cm} (2.3)

The linear part of $G$, and hence of $G_1$, is determined by the linear part of $F$, so by its border polynomials. Obviously the left-hand side of (2.3), and hence its linear part, is determined by the border polynomials of $F$. So equating the linear parts in (2.3) the result follows. \hspace{1cm} \Box

We conclude this paper with a conjecture, which turns out to be equivalent with the Jacobian conjecture. So assume char $k = 0$ from now on.

Substitution of $Y_1 = Y_2 = 0$ in Theorem 1.1 gives:

If $F$ is invertible, then $\frac{d}{dX_1} R_{X_2}(F_1, F_2)$

and $\frac{d}{dX_2} R_{X_1}(F_1, F_2)$ belong to $k^*$.  \hspace{1cm} (2.4)

So if the Jacobian conjecture is true we obtain

**Conjecture 2.5.** If $F$ is a polynomial map, then $\det JF \in k^*$ implies that

$$\frac{d}{dX_1} R_{X_2}(F_1, F_2) \text{ and } \frac{d}{dX_2} R_{X_1}(F_1, F_2) \text{ are in } k^*.$$  \hspace{1cm} (JF is the Jacobian matrix.)
Proposition 2.6. Conjecture 2.5 is equivalent to the Jacobian conjecture.

Proof. It remains to show that Conjecture 2.5 implies the Jacobian conjecture. By [2, Theorem 2.1] it suffices to show that every polynomial map $F$ with $\det JF \in k^*$ is injective. So let $F$ be such a map and assume that $F(a) = F(b)$ for some elements $a$ and $b$ in $k^2$. We have to show that $a = b$. Put $H(X) = F(X + a) - F(a)$. Then $H$ is a polynomial map with $\det JH \in k^*$. Furthermore $H(0) = H(c) = 0$, where $c = b - a$. By Conjecture 2.5, $\det JH \in k^*$ implies that $R_{X_1}(H_1, H_2) = \lambda_1 X_1 + \alpha$ and $R_{X_1}(H_1, H_2) = \lambda_2 X_2 + \beta$ for some elements $\lambda_1$, $\lambda_2$ in $k^*$ and $\alpha$, $\beta$ in $k$. Hence by (0.4) the ideal $(\lambda_1 X_1 + \alpha, \lambda_2 X_2 + \beta)$ is contained in $(H_1, H_2)$, which implies that $H_1$ and $H_2$ have only one zero in common. So $c = 0$, which gives $a = b$, as desired. \qed

References