BULL. AUSTRAL. MATH. SOC. 30C10
VOL. 68 (2003) [73–79]

POLYNOMIAL REMAINDERS AND PLANE AUTOMORPHISMS

TAKIS SAKKALIS

This note relates polynomial remainders with polynomial automorphisms of the plane. It also formulates a conjecture, equivalent to the famous Jacobian Conjecture. The latter provides an algorithm for checking when a polynomial map is an automorphism. In addition, a criterion is presented for a real polynomial map to be bijective.

1. INTRODUCTION

Let $f(x,y), g(x,y)$ be polynomials with coefficients in the field of complex numbers $\mathbf{C}$, of (total) positive degrees n and m, respectively. Consider the map $F := (f,g) : \mathbf{C}^2 \to \mathbf{C}^2$. Let $J(F) = f_x g_y - f_y g_x$ be the determinant of the Jacobian matrix of F. F is called a polynomial automorphism if it has a global polynomial inverse. In this case, an application of the chain rule and the fact that every nonconstant polynomial over $\mathbf{C}$ has a root, implies that $J(F)$ is a nonzero constant. The Jacobian conjecture is that the converse is true. It is also known as Keller's problem, since it first appeared in the literature in [**3**], in which he proves the complex birational case.

In this note, we shall relate polynomial remainders and polynomial automorphisms. In addition, we shall formulate a conjecture which is equivalent to the Jacobian conjecture. The latter provides a relatively easy algorithmic way of checking when a polynomial map f is an automorphism. We conclude with a criterion for a real polynomial map to be bijective.

2. POLYNOMIAL REMAINDERS AND AUTOMORPHISMS

POLYNOMIAL REMAINDERS. Let $p(x_1,\dots,x_n) \in \mathbf{C}[x_1,\dots,x_n]$ of (total) degree k. We say that p is *regular* in x_i, for some $1 \leqslant i \leqslant n$, if $\deg_{x_i} p = k$.

Let F, n, m be as above. We may, after a linear change of coordinates, assume that f, g are regular in x, and of the form

$$\begin{aligned} f(x,y) &= x^n + a_1(y)x^{n-1} + \cdots + a_{n-1}(y)x + a_n(y) \\ g(x,y) &= x^m + b_1(y)x^{m-1} + \cdots + b_{m-1}(y)x + b_m(y) \end{aligned} \tag{1}$$

Received 19th November, 2002

Now suppose that F satisfies the Jacobian condition

$$J(F) = f_x g_y - f_y g_x = 1 \tag{2}$$

Let $f_n(x,y), g_m(x,y)$ be the homogeneous terms of f, g of degrees n, m, respectively. Since $J(F) = 1$, we get that [5],

$$f_n^m = g_m^n \tag{3}$$

Note that $H = (f, g - f)$ satisfies (2). Therefore, in the case where $n = m$, we may replace $g - f$ by g, and assume that $m < n$ and f, g are of the form (1).

Now we observe that $a_1(y) = a^1 y + a^2$ and $b_1(y) = b^1 y + b^2$. We may, after a linear change of coordinates, assume that

$$a_1'(y) = a^1 \neq 0, \quad \text{and} \quad b_1'(y) = b^1 \neq 0$$

To see that, let

$$f_n(x,y) = x^n + a^1 y x^{n-1} + \text{lower degree terms in } x$$
$$g_m(x,y) = x^m + b^1 y x^{m-1} + \text{lower degree terms in } x$$

Condition (3) implies that $n(x^{m-1})^{n-1} \cdot b^1 y = m(x^{n-1})^{m-1} \cdot a^1 y$ and thus $nb^1 = ma^1$. Therefore, in the case where $b^1 = 0$–and thus $a^1 = 0$–, we may replace x with $x + y$ and y with y to get $b^1 = m$ and $a^1 = n$. Then, the polynomials f_x, f_y, g_x, g_y are all regular in x. Now, consider the resultant of g_x and g_y with respect to x,

$$\text{Res}_x(g_x, g_y) = -g_x B + g_y A = c$$

where $A, B \in \mathbf{C}[x,y]$ of degrees–(in x)–at most $m - 2$. Since $J(F) = 1$, we see that c is a non zero constant. Replace A/c with A and B/c with B. The latter, together with (2), gives

$$g_y(f_x - A) = g_x(f_y - B)$$

Since no factor of g_x divides g_y, we see that g_x divides $f_x - A$ and thus we get

$$\begin{aligned} f_x &= g_x h + A \\ f_y &= g_y h + B \end{aligned} \tag{4}$$

for some $h \in \mathbf{C}[x,y]$. Note in the above that $\deg_x B, \deg_x A \leqslant m - 2$. Therefore, A and B are nothing but the *remainders* of the division of f_x by g_x and f_y and g_y, respectively, where the above polynomials are thought of as members of the ring $\mathbf{R}[y][x]$. For notational purposes, we denote $A = \text{rem}_x(f_x, g_x)$ and $B = \text{rem}_x(f_y, g_y)$.

Plane Automorphisms. Suppose now that $F : \mathbf{C}^2 \to \mathbf{C}^2$ is an automorphism. Then in this case it is possible to precisely find what the polynomials A and B look like. Indeed, since F is an automorphism, we see that m divides n and thus $n = mk$, [**4**]. Note that $F_1 = (g, f - g^k)$ is also an automorphism with $\deg(f - g^k) < \deg f$. Using an inductive procedure, we may find a polynomial $\phi(t) \in \mathbf{C}[t]$,

$$\phi(t) = t^k + c_1 t^{k-1} + \cdots + c_{k-1} t$$

so that

$$\deg\bigl(f - \phi(g)\bigr) < m = \deg g$$

Note that $G = \bigl(g, f - \phi(g)\bigr)$ is also a polynomial automorphism with $J(G) = -1$. Also we have:

$$f_x = g_x\,\phi'(g) + \bigl(f_x - g_x\phi'(g)\bigr)$$
$$f_y = g_y\,\phi'(g) + \bigl(f_y - g_y\phi'(g)\bigr) \tag{5}$$

In the above we have:

$$\deg\bigl((f_x - g_x\phi'(g)\bigr) \leqslant m - 2,$$
$$\deg\bigl(f_y - g_y\phi'(g)\bigr) \leqslant m - 2$$

The above, combined with (4), gives us the nature of the polynomials A and B:

$$A = f_x - g_x\phi'(g) = \bigl(f - \phi(g)\bigr)_x$$
$$B = f_y - g_y\phi'(g) = \bigl(f - \phi(g)\bigr)_y \tag{6}$$

Notice that in this case, A and B can also be obtained as follows: Since $F = (f, g)$ is an automorphism, f and g are both regular in x and y, [**4**], and thus if we set $\mathcal{A} = \mathrm{rem}_x(f_x, g_x)$ and $\mathcal{B} = \mathrm{rem}_y(f_y, g_y)$, a degree comparison shows that $A = \mathcal{A}$ and $B = \mathcal{B}$.

The PR Conjecture. From (6) we observe that

$$A_y = B_x \tag{7}$$

With the aid of the above we can formulate the following conjecture and show that it is equivalent to the Jacobian conjecture.

The Polynomial Remainder Conjecture. Suppose that $F, f_x, g_x, f_y, g_y, n, m$ are as above with $m < n$, f, g, f_x, g_x, f_y, g_y regular in x and $J(F) = 1$. Suppose also that $A = \mathrm{rem}_x(f_x, g_x)$, $B = \mathrm{rem}_x(f_y, g_y)$. Then, $A_y = B_x$.

Theorem 2.1. *The polynomial remainder conjecture is equivalent to the Jacobian conjecture.*

Proof: In view of (7), it only suffices to show that the polynomial remainder conjecture implies the Jacobian conjecture. Indeed the condition $A_y = B_x$ combined with (4) gives us $J(g, h) = 0$. Since $J(f, g) = 1$ we get that $h = \psi(g)$ for some $\psi(t) \in \mathbf{C}[t]$, [**2**]. Then

$$A = f_x - g_x\,\psi(g)$$
$$B = f_y - g_y\,\psi(g)$$

https://doi.org/10.1017/S0004972700037424 Published online by Cambridge University Press

Now let $\phi(t) = \int \psi(t)\,dt$ and consider $P(x,y) = f - \phi(g)$. Then,

$$P_x = A, \quad \text{and} \quad P_y = B$$

Notice that $J(F) = J(f - \phi(g), g) = 1$, and thus [**2**, Lemma 9] shows that $\deg_x\bigl(f - \phi(g)\bigr) = \deg\bigl(f - \phi(g)\bigr)$. Let now $k = \deg \phi(t)$. Since $\deg_x\bigl(f - \phi(g)\bigr) = \deg_x A + 1 < m$, we see that the degree of $\phi(g)$ kills the degree of f. Therefore, $n - mk = 0$ and thus m divides n. Repeating the procedure for the map $\bigl(g, f - \phi(g)\bigr)$ and using simple induction on n, it is easily seen, [**4**, Theorem 6, p. 101] that F is a polynomial automorphism. ∎

3. A Decision Procedure for a Map to be Bijective

In this section we shall first state an algorithm for deciding whether a polynomial map F over $\mathbf{C}^2$ is an automorphism. Cheng and Wang in [**1**], have also given such an algorithm which is based on that fact that F is an automorphism if $J(F) = c \neq 0$ and F is injective on a line. Ours, on the other hand, is solely based on remainder sequences and it is motivated by the PR conjecture. In addition, we shall give a criterion for a polynomial map over $\mathbf{R}^2$ to be a homeomorphism.

The Complex Case. Let $F = (f,g) : \mathbf{C}^2 \to \mathbf{C}^2$ be a polynomial map. Suppose that the following (double) polynomial remainder sequence A^i, B^i, $i = 1, 2, \ldots, k$ can be created as follows:

1. $A^1 = \operatorname{rem}_x(f_x, g_x)$, $B^1 = \operatorname{rem}_y(f_y, g_y)$
2. If $A^1_y = B^1_x$, we set $A^2 = \operatorname{rem}_x(g_x, A^1)$ and $B^2 = \operatorname{rem}_y(g_y, B^1)$
3. Assume that $A^1, A^2, \ldots, A^j$, $B^1, \ldots, B^j$ $j \geqslant 2$ have been defined. If $A^j_y = B^j_x$, we set $A^{j+1} = \operatorname{rem}_x(A^{j-1}, A^j)$ and $B^{j+1} = \operatorname{rem}_y(B^{j-1}, B^j)$
4. The sequence ends where one of A^k, B^k is a constant different than zero.

Observe that a necessary condition for the construction of such a sequence is that $\deg_x g_x \leqslant \deg_x f_x, \deg_y g_y \leqslant \deg_y f_y$, and f, f_x, A^j, are regular in x and f, f_y, B^j are regular in y. We then have:

Theorem 3.1. *Suppose $F = (f,g) : \mathbf{C}^2 \to \mathbf{C}^2$ is a polynomial map with $m = \deg g \leqslant n = \deg f$ and $J(F) = c \neq 0$. Then F is an automorphism if and only a sequence A^j, B^j can be created as above.*

Proof: ($\Leftarrow$) From the proof of Theorem 2.1 we see that there exist polynomials $P^j(x,y), j = 1, \ldots, k$ so that:

(1) $P^j_x = A^j, P^j_y = B^j$,

(2) $\deg_x P^1 < \deg_x g, \deg_x P^{j+1} < \deg_x P^j, j = 2, \ldots, k-1$, $\deg_y P^1 < \deg_y g, \deg_y P^{j+1} < \deg_y P^j, j = 2, \ldots, k-1$.

Now, let $F^1 = (g, P^1)$, $F^j = (P^j, P^{j+1}), j = 1, \ldots, k-1$. It is easy to see that $J(F^j) = \pm 1$ and F is an automorphism if and only F^j is an automorphism, $j = 1, \ldots, k-1$. Finally, let us look at $F^{k-1} = (P^{k-1}, P^k)$. Since $\min\{\deg_x P^k, \deg_y P^k\} = 1$ and $J(F^{k-1}) = \pm 1$, we may assume that $P^k(x,y) = ax + by + c$. Then, [**2**, Lemma 19, p. 9] shows that this last map F^{k-1} is an automorphism.

($\Rightarrow$) From the discussion proceeding (6) we see that polynomials $A^1 = \operatorname{rem}_x(f_x, g_x)$ $B^1 = \operatorname{rem}_y(f_y, g_y)$ can be defined and they satisfy $A^1_y = B^1_x$. In addition, the proof of Theorem 2.1 shows that there exists a polynomial $P(x,y)$ of degree less than m so that (g, P) is an automorphism. Since g, P are regular in x and y, a repetition of the above procedure produces the required sequence A^j, B^j. ∎

Suppose now that f, g are regular in x, y, and let u, v be indeterminates. Consider

$$\begin{aligned} A(x,u,v) &= \operatorname{Res}_y(f-u, g-v) = A_k(u,v)x^k + \cdots + A_1(u,v)x + A_0(u,v) \\ B(y,u,v) &= \operatorname{Res}_x(f-u, g-v) = B_r(u,v)y^r + \cdots + B_1(u,v)y + B_0(u,v) \end{aligned} \tag{8}$$

In [**5**, Lemma 1, p. 479, Proposition 1, p. 480] a simple theoretical criterion and formula for the inversion of $F = (f,g)$ is given in terms of $A(x,u,v), B(y,u,v)$, which for the sake of completeness we shall state it here, along with a new proof that will serve as a motivation for the real case.

PROPOSITION 3.1. *Let $F = (f,g) : \mathbf{C}^2 \to \mathbf{C}^2$ with f, g regular in x, y. Then F is an automorphism if and only if $A(x,u,v) = ax + A_0(u,v)$ and $B(y,u,v) = by + B_0(u,v)$, where $a, b \in \mathbf{C}$, $ab \neq 0$. In that case the inverse $F^{-1}(x,y) = (-A_0(x,y)/a, -B_0(x,y)/b)$.*

PROOF: ($\Rightarrow$) In view of [**5**, Theorem 1, p. 475] we see that $k \geqslant 1$. We shall first show that A_k is a non zero constant. For if not, there exists a $z_0 = (u_0, v_0)$ so that $A_k(z_0) = 0$. Then, in this case either $A_k(z_0) = \cdots = A_0(z_0) = 0$ or there exists $r < k$ such that $A_r(z_0) \neq 0$. In the first case, $f - u_0$ and $g - v_0$ would have a common factor of positive degree, a contradiction to F being one to one. In the second case, by the lifting property of the resultant, [**5**, Property 2, p.474], it follows that there exists a sequence $\{z_j\}$ so that $|z_j| \to \infty$ and $F(z_j) \to z_0$, again a contradiction to F being a proper map. Finally, if $k > 1$ we see that this contradicts the fact that F is one to one.

($\Leftarrow$) From (8) we observe that $A(x,f,g) = B(y,f,g) = 0$, and thus $ax + A_0(f,g)$ $= 0$, $by + B_0(f,g) = 0$, and upon solving for x, y the desired result follows. ∎

THE REAL CASE. Suppose now that $f(x,y), g(x,y) \in \mathbf{R}[x,y]$ and consider $F = (f,g) :$ $\mathbf{R}^2 \to \mathbf{R}^2$. In this paragraph we are going to give a somewhat similar criterion to the above for F to be a homeomorphism.

Suppose first that F is a homeomorphism. Note that F is a proper map [a map is proper if the inverse image of a compact set is compact]. Also F is locally one to one, and thus its Jacobian $J(F)(x,y)$ does not change sign over $\mathbf{R}^2$. With loss of little generality, we shall here deal with the case where $J(F)(x,y)$ is a real non vanishing polynomial over $\mathbf{R}^2$.

PROPOSITION 3.2. *Let $F = (f,g) : \mathbf{R}^2 \to \mathbf{R}^2$ be a real polynomial map with f, g regular in y, and $J(F)$ a non constant and non vanishing polynomial over $\mathbf{R}^2$. Then*

F is a homeomorphism of $\mathbf{R}^2$ onto $\mathbf{R}^2$ if and only if either A_k is equal to a nonzero constant, or A_k does not change sign in $\mathbf{R}^2$, and if it vanishes at $w_0 = (u_0, v_0)$, then either $A_j(w_0) = 0$ for $j = 0, \dots, k$ or there exists an $r < k$ with $A_r(w_0) \neq 0$ and near w_0, A_k and A_r have the same sign and $k = r \bmod 2$.

PROOF: ($\Rightarrow$) As in the complex case, we observe that $k \geqslant 1$. Now suppose that A_k vanishes at $w_0 = (u_0, v_0)$ and A_k and A_r have different signs near w_0 and/or $k \neq r \bmod 2$. Let N be a disk around w_0 so that $A_r \neq 0$ on N. In the first case, for any $b > 0$, the image of the map $A : N \times [b, \infty] \to \mathbf{R}$, $A(u, v, x) = A(x, u, v)$ contains 0, and thus by the lifting property of the resultant and the fact that F is a homeomorphism, there exists a real sequence $\left|(x_j, y_j)\right| \to \infty$ and $F(x_j, y_j) \to w_0$. But this contradicts the fact that F is proper. The case where $k \neq r \bmod 2$ is treated similarly. Finally, in the case where $A_j(w_0) = 0$ for $j = 0, \dots, k$, note that the number of such points w_0 is finite, since any such w_0 corresponds to a non trivial factor of $J(F)$.

($\Leftarrow$) Now suppose that A_k is a non zero constant and let K be a compact subset of $\mathbf{R}^2$. Consider the set $M = \left\{x \in \mathbf{R} \mid A(x, u, v) = 0,\ (u, v) \in K\right\}$. Since A_k is a non zero constant, M is a compact subset of $\mathbf{R}$. In addition, since f, g are both regular in y, the set $\left\{(x, y) \in \mathbf{R}^2 \mid F(x, y) = z,\ z \in K\right\}$ is also compact. The latter implies that F is a proper map, and since F is locally one to one, we deduce that F is a homeomorphism of $\mathbf{R}^2$ onto $\mathbf{R}^2$. Finally, the case where K contains a zero of A_k is treated similarly. ∎

EXAMPLE 1. *Let*

$$f = x + y + (x - y)^3,$$
$$g = x - y - (x + y)^3.$$

Then, $J(F) = -18(x^2 - y^2)^2 - 2$ *and*

$$A(x, u, v) = 512x^9 - 192(u - v)x^6 + 384x^5 - 288(u + v)x^4 + (24v^2 + 24u^2 + 168uv)x^3 + (24u - 24v)x^2 + (-18u^2 + 8 + 18v^2)x + (-u^3 - 4v - 4u - 3v^2u + 3u^2v + v^3).$$

EXAMPLE 2. *Let*

$$f = (y + y^3)(1 + (x + y)^2 + y^2),$$
$$g = (x + y + (x + y)y^2)(1 + (x + y)^2 + y^2).$$

Then,

$$J(F) = -(1 + y^2)(1 + x^2 + 2xy + 2y^2)(5x^2y^2 + 3x^2 + 10y^3x + 6xy + 1 + 10y^4 + 9y^2),$$

and

$$A(x, u, v) = (32u^4 + 32u^2v^2)x^5 + (32v^4 + 96u^2v^2 - 128u^3v - 64uv^3 + 64u^4)x^3 + (-128uv^3 + 32v^4 - 128u^3v + 192u^2v^2 + 32u^4)x + (-32v^5 + 32u^5 - 160u^4v + 320u^3v^2 - 320u^2v^3 + 160uv^4).$$

It is easily seen that in both examples $F = (f, g)$ satisfies the conditions of the above Proposition, and thus F is a homeomorphism of $\mathbf{R}^2$ onto $\mathbf{R}^2$.

References

[1] C. Cheng and S. Wang, 'An algorithm that determines whether a polynomial map is bijective', in *Automorphisms of Affine Spaces*, (A. van den Essen, Editor) (Kluwer Academic Publishers, Netherlands **123**, 1995), pp. 169–176.

[2] C. Ching-An Cheng, J. McKay and S. Sui-Sheng Wang, 'Younger mates and the Jacobian conjecture', *Proc. Amer. Math. Soc.* **123** (1995), 2939–2947.

[3] O.H. Keller, 'Ganze Cremona-Tranformationen', *Monatshefte der Mathematischen Physik* **47** (1939), 299–306.

[4] J.H. McKay and S. Sui-Sheng Wang, 'An elementary proof of the automorphism theorem in two variables', *J. Pure Appl. Algebra* **52** (1988), 91–102.

[5] T. Sakkalis, 'On relations between Jacobians and resultants of polynomials in two variables', *Bull. Austral. Math. Soc.* **47** (1993), 473–481.

Department of Mathematics
Agricultural University of Athens
Athens 118 55
Greece
e-mail: takis@aua.gr