<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Test polynomials, retracts, and the Jacobian conjecture</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Shpilrain, V; Yu, JT</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Contemporary Mathematics, 2005, v. 369, p. 253-259</td>
</tr>
<tr>
<td><strong>Issued Date</strong></td>
<td>2005</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10722/75406">http://hdl.handle.net/10722/75406</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.; First published in [Contemporary Mathematics] in [2005, v. 369], published by the American Mathematical Society</td>
</tr>
</tbody>
</table>
Test polynomials, retracts, and the Jacobian conjecture

Vladimir Shpilrain

and

Jie-Tai Yu*

Abstract. Let $K[x, y]$ be the algebra of two-variable polynomials over a field $K$. A polynomial $p = p(x, y)$ is called a test polynomial for automorphisms if, whenever $\varphi(p) = p$ for a mapping $\varphi$ of $K[x, y]$, this $\varphi$ must be an automorphism. Here we show that $p \in \mathbb{C}[x, y]$ is a test polynomial if and only if $p$ does not belong to any proper retract of $\mathbb{C}[x, y]$. This has the following corollary that may have application to the Jacobian conjecture: if a mapping $\varphi$ of $\mathbb{C}[x, y]$ with invertible Jacobian matrix is “invertible on one particular polynomial”, then it is an automorphism. More formally: if there is a non-constant polynomial $p$ and an injective mapping $\psi$ of $\mathbb{C}[x, y]$ such that $\psi(\varphi(p)) = p$, then $\varphi$ is an automorphism.

1 Introduction

Let $K[x, y]$ be the algebra of two-variable polynomials over a field $K$ of characteristic 0. A subalgebra $R$ of $K[x, y]$ is called a retract if there is an idempotent homomorphism $\pi$ of $K[x, y]$ (called a retraction or a projection) such that $\pi(K[x, y]) = R$.

There are several equivalent descriptions of retracts of $K[x, y]$ known by now:

(i) $K[x, y] = R \oplus I$ for some ideal $I$ of $K[x, y]$;

(ii) $K[x, y]$ is a projective extension of $R$ in the category of $K$-algebras;

(iii) By a theorem of Costa [2], every proper retract of $K[x, y]$ (i.e., one different from $K[x, y]$ and $K$) is of the form $K[p]$ for some $p = p(x, y) \in K[x, y]$. The authors earlier proved [3] that there exists an automorphism of $K[x, y]$ which takes $p(x, y)$ to $x + y \cdot q(x, y)$ for some $q(x, y) \in K[x, y]$, and every polynomial of the form $x + y \cdot q(x, y)$ generates a proper retract of $K[x, y]$.

(iv) (see [3]) $p(x, y)$ generates a retract of $K[x, y]$ if and only if there is an endomorphism of $K[x, y]$ which takes $p(x, y)$ to $x$.

(v) (see [3]) $p(x, y)$ belongs to a proper retract of $\mathbb{C}[x, y]$ if and only if $p(x, y)$ is fixed by some endomorphism of $\mathbb{C}[x, y]$ with nontrivial kernel.

Recently retracts have found another application in a general setup of arbitrary free algebras and groups in relation with test elements, introduced in [3]. In general,
an element \( g \) of a group or an algebra \( F \) is a test element if any endomorphism of \( F \) fixing \( g \) is actually an automorphism. It is easy to see that a test element does not belong to any proper retract of \( F \); a remarkable result of Turner [10] says that, if \( F \) is a free group, then the converse is also true. Thus, an element of a free group \( F \) is a test element if and only if it does not belong to any proper retract of \( F \).

Here we establish a similar characterization of test polynomials in \( \mathbb{C}[x,y] \):

**Theorem 1.** A polynomial \( p \in \mathbb{C}[x,y] \) is a test polynomial if and only if \( p \) does not belong to any proper retract of \( \mathbb{C}[x,y] \).

Our proof uses several recent results, in particular, a result of Drensky and Yu [3] mentioned in the item (v) above. Crucial for our proof is the following result of independent interest.

**Theorem 2.** Let \( \varphi \) be an injective endomorphism of \( \mathbb{C}[x,y] \) which is not an automorphism. Suppose that \( \varphi(p) = p \) for some non-constant polynomial \( p \in \mathbb{C}[x,y] \). Then \( p \in \mathbb{C}[q] \), where \( q \) is a coordinate polynomial of \( \mathbb{C}[x,y] \). In particular, \( p \) belongs to a proper retract of \( \mathbb{C}[x,y] \).

Recall that \( q = q(x,y) \) is a coordinate polynomial of \( \mathbb{C}[x,y] \) if it can be taken to \( x \) by an automorphism of \( \mathbb{C}[x,y] \).

We also use results of Shestakov and Umirbaev [7] on estimating degrees of polynomials in two-generated subalgebras of \( K[x,y] \). Another ingredient is a result of Kraft [5] concerning the subalgebra \( \varphi^\infty(\mathbb{C}[x,y]) = \cap_{k=1}^\infty \varphi^k(\mathbb{C}[x,y]) \).

Theorems 1, 2 have the following corollary:

**Corollary.** Let \( \varphi \) be an endomorphism of \( \mathbb{C}[x,y] \) with invertible Jacobian matrix. If there is a non-constant polynomial \( p \in \mathbb{C}[x,y] \) and an injective mapping \( \psi \) such that \( \psi(\varphi(p)) = p \), then \( \varphi \) is an automorphism of \( \mathbb{C}[x,y] \).

This strengthens our earlier result [9, Corollary 1.7], where we showed that, if \( \varphi \) has invertible Jacobian matrix, then \( \varphi(p) = p \) implies that \( \varphi \) is an automorphism of \( \mathbb{C}[x,y] \).

To conclude the Introduction, we raise a problem motivated by results of this paper:

**Problem.** Suppose \( p \in \mathbb{C}[x,y] \) is a test polynomial and \( \varphi \) is an injective mapping of \( \mathbb{C}[x,y] \). Is \( \varphi(p) \) necessarily a test polynomial?

It is interesting to note that, by a result of Jelonek [4], a “generic” polynomial of degree \( \geq 4 \) is a test polynomial.

### 2 Proof of Theorem 2

We consider the following two principal cases.

**Case I.** There is a coordinate polynomial in \( \varphi(\mathbb{C}[x,y]) \).
Case II. There are no coordinate polynomials in $\varphi(\mathbb{C}[x, y])$.

In Case I, consider two subcases:

(1) $\varphi$ is not birational, i.e., does not induce an automorphism of the field of fractions.

Then, by a result of Kraft [5, Lemma 1.3], $\varphi^\infty(\mathbb{C}[x, y])$ is either $\mathbb{C}$ or $\mathbb{C}[f]$, where $f = f(x, y)$ is some polynomial. Obviously, if $\varphi(p) = p$, then $p \in \varphi^\infty(\mathbb{C}[x, y])$. We are therefore going to focus on the case $\varphi^\infty(\mathbb{C}[x, y]) = \mathbb{C}[f]$ and show that, if $\varphi$ is injective, then $p \in \mathbb{C}[q]$, where $q$ is a coordinate polynomial.

Now suppose $r = r(x, y)$ is a coordinate polynomial in $\varphi(\mathbb{C}[x, y])$, and let $r = \varphi(s(x, y))$. Then, since $\varphi$ is injective, the polynomial $s = s(x, y)$ must be coordinate, too, by the result of [1]. Therefore, upon changing generating set of $\mathbb{C}[x, y]$ if necessary, we may assume that $r = \varphi(x)$. Furthermore, we can replace $\varphi$ with its conjugate by an arbitrary automorphism, say $\alpha$, i.e., with $\psi = \alpha \varphi \alpha^{-1}$, and at the same time replace $p$ with $p_1 = \alpha(p)$. Then we have:

$$\psi(p_1) = \alpha \varphi \alpha^{-1}(\alpha(p)) = \alpha(p) = p_1.$$

Therefore, the pair $(\psi, p_1)$ has the same properties that the pair $(\varphi, p)$ does, namely, $\psi$ is injective but not birational, and $\psi(p_1) = p_1$; in particular, $p_1 \in \psi^\infty(\mathbb{C}[x, y])$. By choosing $\alpha$ appropriately, we can also have $\psi(x) = x$, thus getting $x \in \psi^\infty(\mathbb{C}[x, y])$.

Then, if $p$ (and therefore $p_1$) does not belong to $\mathbb{C}[q]$ for any coordinate polynomial $q$, $\psi^\infty(\mathbb{C}[x, y])$ cannot be of the form $\mathbb{C}[f]$, which is in contradiction with the result of Kraft mentioned above. This completes case (1).

(2) $\varphi$ is birational, i.e., induces an automorphism of the field of fractions. Again, as in the case (1) above, we deduce from [1] that $\varphi$ must take some coordinate polynomial to coordinate. Thus, upon changing generating set of $\mathbb{C}[x, y]$ if necessary, we may assume that $\varphi$ takes $x$ to $u$, and $y$ to $v \cdot f(u)$, where $\mathbb{C}[u, v] = \mathbb{C}[x, y]$, and $f(u)$ is a non-constant polynomial (otherwise, $\varphi$ would be an automorphism).

Now let

$$p = p(x, y) = \sum_{i,j} c_{ij} x^i y^j.$$

Then

$$\varphi(p) = \sum_{i,j} c_{ij} u^i v^j (f(u))^j.$$

Let $x^s y^s$ be the highest term of $p(x, y)$ in the “pure lex” order with $y > x$. Then in $\varphi(p)$, the highest term is that of $\varphi(x^s y^s)$ because the $y$-degree of $\varphi(y)$ is not lower than that of $\varphi(x)$. Furthermore, the highest term of $\varphi(x^s y^s)$ must have the $y$-degree at least $s$ since otherwise, one would have both $u$ and $v$ of $y$-degree equal to 0, which is impossible.

If the $y$-degree of $\varphi(x^s y^s)$ is $> s$, this gives a contradiction with $\varphi(p) = p$. Now suppose the $y$-degree of $\varphi(x^s y^s)$ is exactly $s$. This is only possible if the $y$-degree of $v$
Proof. The proof here is based on a result of Shestakov and Umirbaev [7, Theorem 3]. Let $N = N(p,q) = \min_{g.c.d.(n,m)} - m - n + \deg(D(p,q)) + 2$. Following [7], we may

\[ \sum_{i,j} c_{ij} x^i y^j = \sum_{i,j} c_{ij} x^i(y + g(x))^j f(x)^j. \]

Again we use the “pure lex” order with $y > x$ to focus on the monomial of highest degree on either side, but this time we compare the $x$-degrees of these highest-degree monomials. We see that these $x$-degrees cannot be equal unless $f(x)$ is a constant, contradicting the assumption. This completes the proof in Case I.

In Case II, we are going to prove the following somewhat stronger statement:

**Proposition.** Let $\varphi$ be an injective endomorphism of $\mathbb{C}[x,y]$, and suppose that there are no coordinate polynomials in $\varphi(\mathbb{C}[x,y])$. Then $\varphi^\infty(\mathbb{C}[x,y]) = \mathbb{C}$.

**Proof.** Let $\varphi(x) = u = u(x,y)$, $\varphi(y) = v = v(x,y)$, and let $D(u,v)$ denote the determinant of the Jacobian matrix of $\varphi$. Since $\varphi$ is injective, $D(u,v) \neq 0$. Now there are two cases:

1. $\deg(D(u,v)) = 0$, i.e., $D(u,v)$ is a non-zero constant. Then, by a result of Kraft [5], we have $\varphi^\infty(\mathbb{C}[x,y]) = \mathbb{C}$.
2. $\deg(D(u,v)) > 0$. Note that for any $k \geq 1$, there are no coordinate polynomials in $\varphi^k(\mathbb{C}[x,y])$. Indeed, if there were a coordinate polynomial in $\varphi^k(\mathbb{C}[x,y])$, then, by the result of [4], there would have to be a coordinate polynomial in $\varphi^{k-1}(\mathbb{C}[x,y])$. This would lead to a contradiction with the assumption that there are no coordinate polynomials in $\varphi(\mathbb{C}[x,y])$.

Let $\varphi^k(x) = u^{(k)}$, $\varphi^k(y) = v^{(k)}$. Then from $\deg(D(u,v)) > 0$ and from the “chain rule” we get $\deg(D(u^{(k)}, v^{(k)})) \geq k$. Now the Proposition will follow from the lemma below. Before we get to it, we need one more definition.

We call a pair $(p,q)$ of polynomials from $K[x,y]$ **elementary reduced** if the sum of their degrees cannot be reduced by a (non-degenerate) linear transformation or a transformation of one of the following two types:

(i) $(p,q) \rightarrow (p + \mu \cdot q, q)$ for some $\mu \in K^*$; $k \geq 2$;

(ii) $(p,q) \rightarrow (p,q + \mu \cdot p^k)$.

Now we are ready for our

**Lemma.** Let $p = p(x,y)$ and $q = q(x,y)$ be two algebraically independent polynomials such that the pair $(p,q)$ is elementary reduced. Let $n = \deg(p) < m = \deg(q)$; $m, n \geq 2$, $\deg(D(p,q)) \geq k$. Let $w = w(x,y) \in \mathbb{C}[p,q])$. Then, unless $w$ is a linear combination of $p$ and $q$, one has $\deg(w) > \min(n,k)$.

**Proof.** The proof here is based on a result of Shestakov and Umirbaev [7, Theorem 3]. Let $N = N(p,q) = \min_{g.c.d.(n,m)} - m - n + \deg(D(p,q)) + 2$. Following [7], we may
assume that the highest homogeneous parts of \( p \) and \( q \) are algebraically dependent; otherwise, \( \deg(w) > n \) is immediate (unless \( w \) is a linear combination of \( p \) and \( q \)). Then \( \frac{mn}{n,m} - m - n \geq 0 \). Indeed, if \( \gcd(n,m) = n \), then the pair \((p, q)\) would not be elementary reduced, contradicting the assumption. If \( \gcd(n,m) < n \), then 
\[
\frac{n}{\gcd(n,m)} \geq 2, \text{ therefore } \frac{mn}{\gcd(n,m)} \geq 2m, \text{ hence } \frac{mn}{\gcd(n,m)} - m - n \geq 0.
\]
Thus, from now on we assume \( N = N(p,q) \) \( \geq \deg(D(p,q)) + 2 \).

Suppose now that the \( y \)-degree of \( w = w(x,y) \) is of the form \( \frac{n}{\gcd(n,m)} \cdot b + r \neq 0 \), where \( 0 \leq r < \frac{n}{\gcd(n,m)} \). Then, by \cite{7} Theorem 3], we have
\[
\deg(w(p,q)) \geq b \cdot N + mr.
\]
If \( b \neq 0 \), this implies \( \deg(w(p,q)) \geq N \geq k + 2 > k \). If \( b = 0 \), then \( r \neq 0 \), implying \( \deg(w(p,q)) \geq m > n \).

It remains to consider the case where the \( y \)-degree of \( w = w(x,y) \) is 0. Then the \( x \)-degree of \( w \) must be nonzero; suppose it is of the form \( \frac{m}{\gcd(n,m)} \cdot b_1 + r_1 \neq 0 \), where \( 0 \leq r_1 < \frac{m}{\gcd(n,m)} \). Then, again by \cite{7} Theorem 3], we have
\[
\deg(w(p,q)) \geq b_1 \cdot N + nr_1.
\]
As before, \( b_1 \neq 0 \) implies \( \deg(w(p,q)) > k \). If \( b_1 = 0 \), then \( r_1 \geq 2 \) because we assume that \( w(x,y) \) is not linear. Then we have \( \deg(w(p,q)) \geq 2n > n \), which completes the proof of the lemma. \( \square \)

Continuing with the proof of the Proposition, we aim at showing that for any integer \( M \), there is an integer \( k \) such that the degree of any polynomial in \( \varphi^k(\mathbb{C}[x,y]) \) is \( > M \). The above lemma “almost” does it if we use it with \( p = \varphi^k(x) = u(k), \ q = \varphi^k(y) = v(k) \), but it has one extra condition on the pair \((p, q)\) to be elementary reduced, whereas a pair \((u(k), v(k))\) may not be elementary reduced. However, if we denote by \((\overline{u}(k), \overline{v}(k))\) an elementary reduced pair obtained from \((u(k), v(k))\) by elementary transformations, we shall have all conditions of the lemma satisfied for this pair while obviously \( \mathbb{C}[\overline{u}(k), \overline{v}(k)] = \mathbb{C}[u(k), v(k)] \). In particular, the inequality \( \deg(D(\overline{u}(k), \overline{v}(k))) \geq k \) follows from the fact that the mapping \( x \to \overline{u}(k), \ y \to \overline{v}(k) \) is a composition of \( \varphi^k \) with an automorphism \( \alpha \) of \( \mathbb{C}[x, y] \) in such a way that \( \alpha \) is applied first. Therefore, the “chain rule” applied to this composition yields \( \deg(D(\overline{u}(k), \overline{v}(k)))= \deg(D(u(k), v(k))) \). Thus, our lemma is applicable to the pair \((\overline{u}(k), \overline{v}(k))\), which completes the proof of the Proposition and therefore of Theorem 2. \( \square \)

3 Proof of Theorem 1 and Corollary

The “only if” part of Theorem 1 follows from a result of \cite{9} rather easily. If \( p = p(x,y) \) belongs to a proper retract \( \mathbb{C}[q] \) of \( \mathbb{C}[x,y] \), then, by \cite{9}, for some automorphism \( \alpha \), \( \alpha(p) \) belongs to \( \mathbb{C}[x + y \cdot u] \) for some polynomial \( u = u(x,y) \). Then the mapping
For the “if” part of Theorem 1, suppose that \( p \) does not belong to any proper retract of \( \mathbb{C}[x, y] \), and let \( \varphi(p) = p \) for some mapping \( \varphi \) of \( \mathbb{C}[x, y] \). Then, by the result of [3], \( \varphi \) must be injective. Then, by our Theorem 2, \( \varphi \) must be an automorphism, hence \( p \) is a test polynomial. \( \square \)

**Proof of Corollary 1.** By way of contradiction, assume that \( \varphi \) is not an automorphism. Then, by our Theorem 2, \( p \in \mathbb{C}[q] \), where \( q \) is a coordinate polynomial of \( \mathbb{C}[x, y] \). Therefore, the composite mapping \( \psi \varphi \) fixes a polynomial \( f(q) \) in \( q \). Then it is easy to see (by looking at the highest degree monomial in \( f(q) \)) that \( \psi(\varphi(q)) = c \cdot q \) for some \( c \in \mathbb{C}^* \), which implies, by the result of [1], that \( \varphi(q) \) is coordinate. A mapping of \( \mathbb{C}[x, y] \) with invertible Jacobian matrix that takes a coordinate polynomial to a coordinate polynomial is obviously an automorphism, a contradiction. \( \square \)

In conclusion, we recall a result of [3] Theorem 1.3 saying that if, for a mapping \( \varphi \) of \( \mathbb{C}[x, y] \) with invertible Jacobian matrix, \( \varphi(x) \) generates a proper retract of \( \mathbb{C}[x, y] \), then \( \varphi \) is an automorphism of \( \mathbb{C}[x, y] \). Then, the case where \( \varphi(x) \) belongs to a proper retract but does not generate it, can be ruled out since in that case, \( \varphi(x) = f(p(x, y)) \), where \( p(x, y) \) generates a proper retract of \( \mathbb{C}[x, y] \), and \( f \) is some one-variable polynomial of degree \( > 1 \). The gradient of such a polynomial cannot form a row of any invertible Jacobian matrix, which can be easily seen from the “chain rule” applied to \( f(p(x, y)) \).

Therefore, by Theorem 1 of the present paper, if \( \varphi \) is a counterexample to the Jacobian conjecture for \( \mathbb{C}[x, y] \), then \( \varphi(x) \) must be a test polynomial. Perhaps a way to prove the Jacobian conjecture for \( \mathbb{C}[x, y] \) could be through showing that the gradient of a test polynomial cannot form a row of any invertible Jacobian matrix. This is known to be the case with (non-commutative) partial derivatives of a test element of a free group of rank 2, see [3] Corollary 2.2.8.

**Acknowledgement**

The first author is grateful to the Department of Mathematics of the University of Hong Kong for its warm hospitality during his visit when most of this work was done.

**References**


Department of Mathematics, The City College of New York, New York, NY 10031
e-mail address: shpil@groups.sci.ccny.cuny.edu
\url{http://www.sci.ccny.cuny.edu/~shpil}

Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong
e-mail address: yujt@hkusua.hku.hk
\url{http://hkumath.hku.hk/~jtyu}