# POLYNOMIAL AUTOMORPHISMS AND GRÖBNER REDUCTIONS

Vladimir Shpilrain and Jie-Tai Yu

Abstract. Let $P_n = K[x_1, ..., x_n]$ be the polynomial algebra over a field $K$ of characteristic 0. We show that applying an automorphism to a given polynomial $p \in P_n$ is mimicked by Gröbner transformations of a basis of the ideal of $P_n$ generated by partial derivatives of this polynomial. In the case of $P_2$, this yields a miraculously simple algorithm for deciding whether or not a given polynomial from $P_2$ is part of a basis. Another application is an algorithm which, given a polynomial $p \in P_2$ which is part of a basis, finds a sequence of elementary automorphisms that reduces $p$ to $x_1$. We also speculate on how our method may be used for constructing a possible counterexample to the Jacobian Conjecture in higher dimensions.

## 1. Introduction

Let $P_n = K[x_1, ..., x_n]$ be the polynomial algebra over a field $K$ of characteristic 0. Define the *outer rank* of a polynomial $p \in P_n$ to be the minimal number of generators $x_i$ on which an automorphic image of $p$ can depend. This has a simple geometric meaning: if the outer rank of a polynomial $p \in P_n$ equals $k$, $k \leq n$, then (in case the ground field $K$ is algebraically closed), in the affine space $\mathbf{A}^n$, the hypersurface $p = 0$ can be mapped (by an automorphism of $\mathbf{A}^n$) onto a cylinder whose base has dimension $k$, and $k$ is minimal with this property.

The present paper was originally motivated by the problem of determining the outer rank of a given polynomial $p$.

This problem has been considered for various algebraic systems. The first significant result should be attributed to Whitehead: based on his powerful combinatorial technique, it is possible to determine the outer rank of an element of a free group – see [10].

Recently, Umirbaev [15] has come up with an observation of major importance: the outer rank of a free group element appears to be equal to the rank (i.e., to the minimal number of generators) of the right ideal of the free group ring generated by partial (non-commutative) Fox derivatives of this element.

In [11], similar result has been proved (independently, but somewhat earlier) for an element of a free Lie algebra.

---

1991 *Mathematics Subject Classification.* Primary 13B25, 13P10; Secondary 14E09.

These results might tempt one to assume that also in the case of a polynomial algebra $P_n$, the outer rank of a polynomial $p$ equals the rank of the ideal of $P_n$ generated by partial derivatives of $p$. This however is not the case as the following example shows. Partial derivatives of the polynomial $p = x_1 + x_1^2 x_2$ generate the whole algebra $P_2$ as an ideal; therefore, they generate an ideal of rank 1 (a *principal* ideal). At the same time, it is easy to see that the outer rank of this polynomial equals 2.

The analysis of this example has led us to the following observation. In the course of constructing a Gröbner basis of a given ideal, one uses "reductions", i.e., transformations of the following type (see [1], p.39-43): given a pair $(p, q)$ of polynomials, set $S(p, q) = \frac{L}{l.t.(p)} \cdot p - \frac{L}{l.t.(q)} \cdot q$, where $l.t.(p)$ is the *leading term* of $p$, i.e., the *leading monomial* together with its coefficient; $L = l.c.m.(l.m.(p), l.m.(q))$ (here, as usual, $l.c.m.$ means the least common multiple, and $l.m.(p)$ denotes the leading monomial of $p$). In this paper, we'll always consider what is called "deglex ordering" in [1] – where monomials are ordered first by total degree, then lexicographically with $x_1 > x_2 > ... > x_n$.

Now a crucial observation is as follows. These Gröbner reductions appear to be of two essentially different types:

(i) *regular*, or *elementary*, transformations. These are of the form $S(p, q) = \alpha \cdot p - r \cdot q$ or $S(p, q) = \alpha \cdot q - r \cdot p$ for some polynomial $r$ and scalar $\alpha \in K^*$. This happens when the leading monomial of $p$ is divisible by the leading monomial of $q$ (or vice versa). The reason why we call these transformations *elementary* is that they can be written in the form $(p,\ q) \to (\alpha_1 p,\ \alpha_2 q) \cdot M$, where $M$ is an *elementary matrix*, i.e., a matrix which (possibly) differs from the identity matrix by a single element outside the diagonal. In case when we have more than 2 polynomials $(p_1, ..., p_k)$, we still can write $(p_1, ..., p_k) \to (\alpha_1 p_1, ..., \alpha_k p_k) \cdot M$, where $M$ is a $k \times k$ elementary matrix; elementary reduction here is actually applied to a pair of polynomials (as usual), while the other ones are kept fixed. Sometimes, it is more convenient for us to get rid of the coefficients $\alpha_i$ and write $(p_1, ..., p_k) \to (p_1, ..., p_k) \cdot M$, where $M$ belongs to the group $GE_k(P_n)$ generated by all elementary **and** diagonal matrices from $GL_k(P_n)$. It is known [14] that $GE_k(P_n) = GL_k(P_n)$ if $k \geq 3$, and $GE_2(P_n) \neq GL_2(P_n)$ if $n \geq 2$ – see [3].

(ii) *singular* transformations – these are non-regular ones.

It appears that the reason why the outer rank of the polynomial $p = x_1 + x_1^2 x_2$ above is greater than the rank of the ideal $I_{d(p)}$ of $P_2$ generated by partial derivatives of $p$, is the *presence of singular transformations* in the corresponding reduction process.

We say that a polynomial $p \in P_n$ has a *unimodular gradient* if $I_{d(p)} = P_n$ (in particular, the ideal $I_{d(p)}$ has rank 1 in this case). Note that if the ground field $K$ is algebraically closed, then this is equivalent, by Hilbert's Nullstellensatz, to the gradient being nowhere-vanishing.

Then we have:

**Theorem 1.1.** *Let a polynomial $p \in P_2$ have a unimodular gradient. Then the outer rank of $p$ equals 1 if and only if one can get from $(d_1(p),\ d_2(p))$ to (1, 0) by using only elementary transformations. Or, in the matrix form: if and only if $(d_1(p),\ d_2(p)) \cdot M = (1,\ 0)$ for some matrix $M \in GE_2(P_2)$.*

Our proof of Theorem 1.1 is based on a generalization of Wright's Weak Jacobian Theorem [16] – see Proposition 2.4.

**Remark 1.2.** Elementary transformations that reduce $(d_1(p),\ d_2(p))$ to $(1,\ 0)$, can be actually chosen to be Gröbner reductions, i.e., to decrease the maximum degree of monomials *at every step* – we prove it based on a recent result of Park (see Proposition 2.5).

Now we show how one can apply this result to the study of so-called coordinate polynomials.

We call a polynomial $p \in P_n$ *coordinate* if it can be included in a generating set of cardinality $n$ of the algebra $P_n$. It is clear that the outer rank of a coordinate polynomial equals 1 (the converse is not true!). It is easy to show that coordinate polynomial has a unimodular gradient, and again – the converse is not true! On the other hand, we have:

**Proposition 1.3.** *A polynomial $p \in P_n$ is coordinate if and only if it has outer rank 1* **and** *a unimodular gradient.*

Combining this proposition with Theorem 1.1 yields the following

**Theorem 1.4.** *A polynomial $p \in P_2$ is coordinate if and only if one can get from $(d_1(p),\ d_2(p))$ to (1, 0) by using only elementary Gröbner reductions.*

This immediately yields an algorithm for detecting coordinate polynomials in $P_2$. Our algorithm is very simple and fast: it has quadratic growth with respect to the degree of a polynomial. In case $p$ is revealed to be a coordinate polynomial, the algorithm also gives a polynomial which completes $p$ to a basis of $P_2$.

In the case when $K = \mathbf{C}$, the field of complex numbers, an alternative, somewhat more complicated algorithm, has been recently reported in [6]. It is not known whether or not there is an algorithm for detecting coordinate polynomials in $P_n$ if $n \geq 3$.

Theorems 1.1 and 1.4 also suggest the following conjecture which is relevant to an important problem known as "effective Hilbert's Nullstellensatz" (see [13]):

**Conjecture "G".** Let a polynomial $p \in P_2$ have a unimodular gradient. Then one can get from $(d_1(p),\ d_2(p))$ to $(1,\ 0)$ by using *at most one* singular Gröbner reduction.

**Remark 1.5.** For $n \geq 3$, Theorem 1.1 is no longer valid since in this case, by a result of Suslin [14], the group $GL_n(P_n) = GE_n(P_n)$ acts transitively on the set of all unimodular polynomial vectors of dimension $n$, yet there are polynomials with unimodular gradient, but of the outer rank 2 – see example above. The "only if" part however is valid for

an arbitrary $n \geq 2$ – see Proposition 2.1. It is also easy to show that one always has $orank\ p \geq rank(I_{d(p)})$ – see Lemma 2.3.

Finally, we show that our method also yields an algorithm which, given a coordinate polynomial $p \in P_2$, finds a sequence of elementary automorphisms (i.e., automorphisms of the form $x_1 \to x_1 + f(x_2);\ x_2 \to x_2$ together with linear automorphisms) that reduces $p$ to $x_1$ – see Remark 3.1.

The arrangement of the paper is as follows. In Section 2, we prove our main results. Then, in Section 3, we give an actual description of the algorithm for detecting coordinate polynomials in $P_2$. In the concluding Section 4, we discuss how our method may be used for constructing a possible counterexample to the Jacobian Conjecture in higher dimensions.

## 2. Proofs

We start by fixing some notation. We write $orank\ p$ for the outer rank of a polynomial $p \in P_n$, and $I_{d(p)}$ for the ideal of $P_n$ generated by partial derivatives $d_1(p), ..., d_n(p)$ of $p$. Naturally, $d_k(p)$ denotes partial derivative of $p$ with respect to $x_k$. For an automorphism $\varphi$ that takes $x_i$ to $p_i$, $1 \leq i \leq n$, the Jacobian matrix is defined as follows: $J_\varphi = (d_j(p_i))_{1 \leq i,j \leq n}$.

We need the "chain rule": if $p = \varphi(q)$ for some endomorphism $\varphi$, then (in the matrix form)

$$(d_1(p), ..., d_n(p)) = (\varphi(d_1(q)), ..., \varphi(d_n(q))) \cdot J_\varphi, \tag{1}$$

where $J_\varphi$ is the Jacobian matrix of $\varphi$. There is also a useful product rule for the Jacobian matrices:

$$J_{\varphi(\psi)} = \psi(J_\varphi) \cdot J_\psi. \tag{2}$$

**Proof of Proposition 1.3.**
(i) Suppose $p$ is coordinate. Then $orank\ p = 1$ since, by definition, there is an automorphism of $P_n$ that takes $p$ to $x_1$.

Now let $p = \varphi(x_1)$ for some automorphism $\varphi$. Then, applying the "chain rule" (1), we get

$$(d_1(p), ..., d_n(p)) = (\varphi(d_1(x_1)), ..., \varphi(d_n(x_1))) \cdot J_\varphi.$$

This gives

$$(d_1(p), ..., d_n(p)) = (1,\ 0, ...,\ 0) \cdot J_\varphi. \tag{3}$$

Since $\varphi$ is an automorphism, the Jacobian matrix $J_\varphi$ is invertible, so that (3) gives

$$(d_1(p), ..., d_n(p)) \cdot J_\varphi^{-1} = (1,\ 0, ...,\ 0),$$

implying $1 \in I_{d(p)}$, so $I_{d(p)} = P_n$.

(ii) Now suppose *orank* $p = 1$, and $I_{d(p)} = P_n$. After applying an automorphism (if necessary), we can reduce $p$ to the form $p = \sum_i \alpha_i\ x_1^i$, where $\alpha_i \in K$. Therefore, $d_1(p)$ should generate the whole $P_n$ as an ideal. But this is only possible if $\alpha_i = 0$ for $i > 1$. Thus, $p$ is coordinate. □

Our next goal is to prove Theorem 1.1. First we prove the "only if" part of this theorem in a more general form:

**Proposition 2.1.** *Let $p \in P_n$ be a coordinate polynomial. Then one can get from $(d_1(p), ..., d_n(p))$ to (1, 0, ..., 0) by using only elementary transformations.*

We need one lemma:

**Lemma 2.2.** *If $\varphi$ is an automorphism of $P_n$, then the Jacobian matrix $J_\varphi$ belongs to $GE_n(P_n)$.*

**Proof.** The fact that $J_\varphi$ belongs to $GL_n(P_n)$, follows from the "chain rule". Now there are 2 cases:
(i) $n \geq 3$. Then we just have $GE_n(P_n) = GL_n(P_n)$ by a result of [14].
(ii) $n = 2$. In this case, the automorphism group of $P_2$ is generated by linear automorphisms together with automorphisms of the form $x_1 \to x_1 + f(x_2);\ x_2 \to x_2$, where polynomial $f(x_2)$ does not depend on $x_1$ (see [4], [7]). It is easy to see that the Jacobian matrix of any of those automorphisms belongs to $GE_2(P_2)$; hence the Jacobian matrix of any automorphism of $P_2$ belongs to $GE_2(P_2)$ as well - this follows from the product rule (2). □

Now we are ready for a
**Proof of Proposition 2.1.**
First of all, $I_{d(p)} = P_n$ by Proposition 1.3. Since $p$ is coordinate, we have $p = \varphi(x_1)$ for some automorphism $\varphi$. Arguing as in the proof of Proposition 1.3, we get

$$(d_1(p), ..., d_n(p)) \cdot J_\varphi^{-1} = (1,\ 0, ...,\ 0). \tag{4}$$

Since $J_\varphi^{-1} \in GE_n(P_n)$ by Lemma 2.2, (4) implies one can get from $(d_1(p), ..., d_n(p))$ to (1, 0, ..., 0) by using only elementary transformations. □

**Proof of Theorem 1.1.**
The "only if" part follows from Proposition 2.1, so we proceed with the "if" part.

Again, we need one general lemma:

**Lemma 2.3.** *For an arbitrary polynomial $p \in P_n$, one has orank $p \geq rank(I_{d(p)})$.*

**Proof.** Let *orank* $p = k$. Then, upon applying an automorphism (if necessary), we can assume that $p$ has the form $p = p(x_1, ..., x_k)$. Note that the rank of $I_{d(p)}$ does not change

under applying an automorphism to $p$ - this is clear from the "chain rule" (1). Now we see that the ideal $I_{d(p)}$ can be generated by $k$ elements. $\square$

Back to the proof of Theorem 1.1, we see that by Lemma 2.3, the only case when we could possibly have $orank\ p \neq rank(I_{d(p)})$, is when $orank\ p = 2$ whereas $rank(I_{d(p)}) = 1$.

Since one can get from $(d_1(p),\ d_2(p))$ to $(1, 0)$ by using only elementary transformations, we have

$$(d_1(p),\ d_2(p)) \cdot M = (1,\ 0)$$

for some matrix $M \in GE_2(P_2)$.

Let $M = \begin{pmatrix} q_1 & r_1 \\ q_2 & r_2 \end{pmatrix}$, so that

$$d_1(p)\ r_1\ +\ d_2(p)\ r_2 = 0. \tag{5}$$

Since $M \in GL_2(P_2)$, the column $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ must be unimodular, i.e., for some polynomials $s_1, s_2 \in P_2$, we have

$$s_1\ r_1\ +\ s_2\ r_2 = 1.$$

This together with (5) gives:

$$\begin{pmatrix} d_1(p) & d_2(p) \\ s_1 & s_2 \end{pmatrix} \cdot M\ =\ \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}\ =\ M_1.$$

The matrix $M_1$ belongs to $GE_2(P_2)$ because it is triangular. Hence the matrix $J\ =\ \begin{pmatrix} d_1(p) & d_2(p) \\ s_1 & s_2 \end{pmatrix}$ belongs to $GE_2(P_2)$, too.

Now we arrive at the most crucial point of the proof. We are going to use a result of [16] (Weak Jacobian Theorem) in a somewhat stronger form. The result itself says: if $p,\ q$ are two polynomials from $P_2$, and the corresponding Jacobian matrix $J = \begin{pmatrix} d_1(p) & d_2(p) \\ d_1(q) & d_2(q) \end{pmatrix}$ belongs to $GE_2(P_2)$, then $p$ and $q$ generate $P_2$; in particular, they both are coordinate polynomials.

A closer look at the (inductive) argument in the proof of this result (see [16, p. 250]), shows that the condition on the *second* row of the matrix $J$ to have the form $(\,d_1(q) \quad d_2(q)\,)$, is not actually used. In other words, the result can be strengthened as follows:

**Proposition 2.4.** *If $J$ is a matrix of the form $\begin{pmatrix} d_1(p) & d_2(p) \\ s_1 & s_2 \end{pmatrix}$, and $J \in GE_2(P_2)$, then $p$ is a coordinate polynomial. Furthermore, there is a polynomial $q \in P_2$ such that $s_1\ =\ d_1(q)$; $s_2\ =\ d_2(q)$, and $p$ and $q$ generate $P_2$.*

**Proof** of this proposition repeats the proof of Theorem 6 from [16] until "the very last moment", when the actual induction step is being done. Since we don't know *a priori* if

our matrix $J$ is the Jacobian matrix of some endomorphism $\varphi$, we cannot talk about composing $\varphi$ with the elementary automorphism $\psi$ constructed in the course of the proof of Theorem 6 in [16, p.250].

Instead, having in mind the product rule (2), we just consider the matrix $J^* = \psi(J) \cdot J_\psi$, where $J_\psi$ is the Jacobian matrix of $\psi$, hence an elementary matrix. The same expansion of $J^*$ as the one of $J_{\psi\varphi}$ in [16, p.250], shows that the "normal form" of $J^*$ has smaller length than that of $J$. Hence we may refer to the inductive assumption as soon as we show that the first row of the matrix $J^*$ still has the form $(\, d_1(q) \quad d_2(q)\,)$ for some polynomial $q \in P_2$.

Indeed, it is straightforward to see that the first row of the matrix $J^*$ is $(\, d_1(\psi(p)) \quad d_2(\psi(p))\,)$. This completes the proof of Proposition 2.4, and the proof of Theorem 1.1 thereby, since we have shown that $p$ is a coordinate polynomial, in particular, $orank\ p = 1$. $\square$

**Proof of Theorem 1.4.**

Our proof is based on the following recent result of H.Park [12] (we give it here in a little stronger form):

**Proposition 2.5.** *Let* $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GE_2(P_2)$, *and* $l.m.(A) = \begin{pmatrix} l.m.(p) & l.m.(q) \\ l.m.(r) & l.m.(s) \end{pmatrix}$ *- the matrix of its leading monomials. Then, either at least 3 of the entries of* $A$ *are constants, or one of the rows of* $l.m.(A)$ *is a monomial multiple of the other row, as well as one of the columns is a monomial multiple of the other column.*

Since the paper [12] is not published yet, we give a brief exposition of the proof.

The proof is by induction on the (minimal) number of elementary matrices $E_i$ in a decomposition of the form

$$A = D \cdot E_1 \cdots E_k,\ k \geq 2,$$

where $D$ is a diagonal matrix, and $E_1 \ldots E_k$ - elementary matrices.

Since the matrix $A$ is invertible, leading terms should cancel out when we compute the determinant of $A$; this means in the matrix $l.m.(A)$, either all of the entries are constants, or one of the entries is 0 and two of the other are constants, or $\det(l.m.(A)) = 0$.

Let $\det(l.m.(A)) = 0$. Denote $A' = D \cdot E_1 \cdots E_{k-1}$, and consider 2 possibilities in accordance with our induction hypothesis.

**(i)** $l.m.(A')$ has 3 constant entries. Let $E_k = \begin{pmatrix} 1 & 0 \\ g & 1 \end{pmatrix}$. There are 3 possibilities (up to a "symmetry") for the matrix $l.m.(A')$:

**(a)** All the entries of $l.m.(A')$ are constants. In this case, the matrix $l.m.(A)$ is of the form $\begin{pmatrix} l.m.(g) & 1 \\ l.m.(g) & 1 \end{pmatrix}$. The result follows.

**(b)** Precisely 3 entries of $l.m.(A')$ are constants. In this case, one of them is 0. Let $l.m.(A') = \begin{pmatrix} f & 1 \\ 1 & 0 \end{pmatrix}$. Then $l.m.(A)$ has 3 constant entries.

**(c)** The same as (b), but $l.m.(A') = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$, $f$ non-constant. Then $l.m.(A) = \begin{pmatrix} l.m.(f)\ l.m.(g) & l.m.(f) \\ l.m.(g) & 1 \end{pmatrix}$, so that the first row of $l.m.(A)$ is $l.m.(f)$ times the second row, as well as the first column is $l.m.(g)$ times the second column.

Now we come to the main case.

**(ii)** Let $A' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and, say,

$$(l.m.(a),\ l.m.(b)) = h \cdot (l.m.(c),\ l.m.(d)); \tag{6}$$

$$(l.m.(a),\ l.m.(c)) = h' \cdot (l.m.(b),\ l.m.(d)) \tag{7}$$

for some non-constant monomials $h$, $h'$ (if some of them is constant, then we are done). This means, in particular, that $a$, $b$, $c$ are non-constant.

Again, we consider only one case here - when $E_k = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}$, $g \neq 0$. Then $A = \begin{pmatrix} a & b+ga \\ c & d+gc \end{pmatrix}$. Since $\det(A) = 1$, this yields

$$l.m.(c) \cdot l.m.(b+ga) = l.m.(a) \cdot l.m.(d+gc) = h \cdot l.m.(c) \cdot l.m.(d+gc).$$

Therefore, $l.m.(b+ga) = h \cdot l.m.(d+gc)$. This together with (6) means the first row of $l.m.(A)$ is $h$ times the second row. Also, by (7), we have $l.m.(b+ga) = l.m.(ga) = l.m.(g) \cdot l.m.(a)$, and $l.m.(d+gc) = l.m.(gc) = l.m.(g) \cdot l.m.(c)$, hence the second column of $l.m.(A)$ is $l.m.(g)$ times the first column.

This completes the proof of Proposition 2.5. □

To complete the proof of Theorem 1.4, we recall from the proof of Theorem 1.1 that polynomial $p$ is coordinate if and only if the row $(d_1(p),\ d_2(p))$ can be completed to a matrix from $GE_2(P_2)$. Combining this with Proposition 2.5 yields the result. □

## 3. Algorithm for detecting coordinate polynomials

Given a polynomial $p = p(x_1, x_2)$, we want to figure out whether or not it is part of a basis of the polynomial algebra $P_2$.

**Step 1.** Take the derivatives $d_1(p)$, $d_2(p)$; denote $q_1 = d_1(p)$, $q_2 = d_2(p)$.

**Step 2.** If the leading monomial (l.m.) of $q_1$ is not divisible by the leading monomial of $q_2$ (or vice versa), then $p$ is **not** a part of a basis - this follows from Theorem 1.1 and Proposition 2.5. If $l.m.(q_1) = h \cdot l.m.(q_2)$ or $l.m.(q_2) = h \cdot l.m.(q_1)$ for some monomial $h$, then we go on to

**Step 3.** Set $q_1' = q_1 - h \cdot q_2$, or $q_2' = q_2 - h \cdot q_1$, respectively. If, say, $l.m.(q_1') = 1$, then $p$ is part of a basis by Theorem 1.1. If $l.m.(q_1') = 0$, then $p$ is part of a basis if

and only if $l.m.(q_2) = 1$ - again by Theorem 1.1. If $l.m.(q_1') \neq 0$ *or* 1, then repeat Step 2 upon replacing $q_1$ with $q_1'$, or $q_2$ with $q_2'$, respectively. $\square$

Since the maximum of the degrees of $q_1$ and $q_2$ decreases every time we apply Step 3, we can apply it at most $d + (d-1) + ... + 1 = d(d+1)/2$ times, where $d$ is the degree of a polynomial $p$. Therefore, our algorithm has quadratic growth with respect to the degree of a polynomial.

If our algorithm has revealed $p$ to be a coordinate polynomial, then it is also easy to find a polynomial $q$ such that $p$ and $q$ generate the whole algebra $P_2$. All we have to do is to keep track of the transformations in Step 3 in the matrix form as follows: $(q_1,\ q_2) \to (q_1,\ q_2)\ E(h)$, where $E(h) = \begin{pmatrix} 1 & 0 \\ -h & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & -h \\ 0 & 1 \end{pmatrix}$. In the end, if the polynomial $p$ is coordinate, we arrive at $(d_1(p),\ d_2(p)) = (1,\ 0) \cdot M$, where $M$ is a product of all the matrices $E(h)$ that we have encountered. It follows that $M$ is of the form $\begin{pmatrix} d_1(p) & d_2(p) \\ s_1 & s_2 \end{pmatrix}$. Then, by Proposition 2.4, we conclude that $s_1 = d_1(q)$; $s_2 = d_2(q)$ for a polynomial $q \in P_2$, and $p$ and $q$ generate $P_2$. $\square$

**Remark 3.1.** This algorithm can be also used to find a sequence of elementary automorphisms that reduces $p \in P_2$ to $x_1$ in case $p$ is a coordinate polynomial. Indeed, as we have just shown, we can find a matrix $M \in GE_2(P_2)$ such that $(d_1(p),\ d_2(p)) = (1,\ 0) \cdot M$, together with a decomposition of $M$ as a product of elementary matrices. Then, applying the inductive argument from the proof of [16, Theorem 6] gives an effective procedure for constructing a desired sequence of elementary automorphisms.

Namely, suppose $M = E_{12}(p_1) \cdot E_{21}(q_1) \cdot ... \cdot E_{12}(p_k) \cdot E_{21}(q_k)$, where $E_{12}(p) = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$, and $E_{21}(q) = \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix}$. Then, from Wright's proof, it follows that $q_k = q_k(x_1)$, so that the matrix $E_{21}(q_k)$ is the Jacobian matrix of an elementary automorphism. Similarly, if the first elementary matrix on the right is of the form $E_{12}(p_k)$, then $p_k = p_k(x_2)$ whence $E_{12}(p_k)$ is the Jacobian matrix of an elementary automorphism. The inductive procedure now is clear. $\square$

**Remark 3.2.** An algorithm alternative to that of Remark 3.1 can be obtained as follows. Given a coordinate polynomial $p \in P_2$, we can find a polynomial $q$ such that $p$ and $q$ generate $P_2$ – see above. Then we can use the procedure based on [4, Theorem 8.5] to reduce $(p,\ q)$ to $(x_1,\ x_2)$ by a sequence of elementary automorphisms. The difference between this algorithm and that of Remark 3.1, is (informally speaking) the same as between Nielsen's and Whitehead's algorithms in a free group (see [10]).

## 4. Relation to the Jacobian Conjecture

In this section, we discuss very briefly how our method may be used to construct a possible counterexample to the Jacobian Conjecture in higher dimensions.

The Jacobian Conjecture is very well-known (see [2], [5] for a survey and background), but just to make the exposition self-contained, we recall its claim:

**Jacobian Conjecture.** If the Jacobian matrix $J = (d_j(p_i))_{1\le i,j\le n}$ is invertible, then polynomials $p_1, \dots, p_n$ generate the whole algebra $P_n$.

First of all, we note:

**Proposition 4.5.** *If polynomials $p_1, \dots, p_n$ provide a counterexample to the Jacobian Conjecture with minimal possible $n$, then each of those polynomials has outer rank bigger than 1.*

**Proof.** Suppose $p_1$, say, has outer rank 1. Then, upon applying an automorphism (if necessary), we can assume that $p_1$ has the form $p_1 = p_1(x_1)$. In order to have the Jacobian matrix invertible, we should have then $p_1 = \alpha \cdot x_1$ for some $\alpha \in K^*$. Then, $(n-1)\times(n-1)$ Jacobian matrix $J' = (d_j(p_i))_{2\le i,j\le n}$ is also invertible, which implies, by the minimality assumption, that $K(x_1)[p_2, \dots, p_n] = K(x_1)[x_2, \dots, x_n]$, where $K(x_1)$ is the quotient field of $K[x_1]$. It follows that $K(x_1, p_2, \dots, p_n) = K(x_1, x_2, \dots, x_n)$, which by Keller's theorem [8] implies $K[x_1, p_2, \dots, p_n] = P_n$. Therefore, polynomials $p_1, \dots, p_n$ generate the whole algebra $P_n$, hence a contradiction. □

This shows that polynomials with unimodular gradient, but of the outer rank bigger than 1, are the key to constructing a counterexample to the Jacobian Conjecture. By a result of Suslin [14], every unimodular polynomial row of dimension $n \ge 3$ can be completed to invertible $n \times n$ matrix over $P_n$. Of course, the problem is to have those other $(n-1)$ rows satisfy the conditions $d_j(q_i) = d_i(q_j)$ for every row $(q_1, \dots, q_n)$ – this is needed to make sure our invertible matrix is actually a Jacobian matrix.

The higher dimension of our unimodular row is, the "more room" we have for building a matrix with desired properties. There are several algorithms known for completing a unimodular polynomial row to invertible square matrix over $P_n$ (see e.g. [9]), but all of them are rather complicated. A practical algorithm like that would be a major step toward constructing a counterexample to the Jacobian Conjecture (if such a counterexample exists).

**Acknowledgement**

We are grateful to H.Park for his kind permission to use his unpublished result (Proposition 2.5) here. The second author also thanks Department of Mathematics of the University of California, Santa Barbara, for its warm hospitality during his visit when this work was initiated.

## References

1. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, V.3, American Mathematical Society, 1994.

2. H. Bass, E. Connell and D. Wright, *The Jacobian conjecture: reduction of degree and formal expansion of the inverse*, Bull. Amer. Math. Soc. **7** (1982), 287–330.
3. P.M.Cohn, *On the structure of the $GL_2$ of a ring*, Inst. Hautes Études Sci. Publ. Math. **30** (1966), 365–413.
4. P.M.Cohn, *Free rings and their relations*, Academic Press, 1985.
5. A. van den Essen, *Seven lectures on polynomial automorphisms*, Automorphisms of Affine Spaces (ed. A. van den Essen), Proc. of the conference 'Invertible Polynomial maps', July 1994, Curaçao, 3-39. Kluwer Academic Publishers, 1995.
6. A. van den Essen, *Locally nilpotent derivations and their applications, III*, J. Pure Appl. Algebra **98** (1995), 15-23.
7. H.W.E.Jung, *Über ganze birationale Transformationen der Ebene*, J. Reine Angew. Math. **184** (1942), 161-174.
8. O. Keller, *Ganze Cremona-Transformationen*, Monatsh. Math. Phys. **47** (1939), 299-306.
9. A. Logar and B. Sturmfels, *Algorithms for the Quillen-Suslin theorem*, J. Algebra **145** (1992), 231–239.
10. R.Lyndon, P. Shupp, *Combinatorial Group Theory*, Series of Modern Studies in Math. **89**. Springer-Verlag, 1977.
11. A. A. Mikhalev and A. A. Zolotykh, *Rank of an element of the free Lie (p-)superalgebra*, Russian Acad. Sci. Dokl. Math. **49** (1994), 189–193.
12. H. Park, *A Computational Theory of Laurent Polynomial Rings and Multidimensional FIR Systems*, PhD thesis, University of California at Berkeley, 1995.
13. M.Shub, S.Smale, *On the intractability of Hilbert's Nullstellensatz and an algebraic version of "$NP \neq P$?"*, Duke Math. J. **81** (1996), 47–54.
14. A. A. Suslin, *On the structure of the special linear group over polynomial rings*, Math. USSR Izv. **11** (1977), 221–238.
15. U.U.Umirbaev, *On the rank of elements of free groups*, Russian Math. Surveys, to appear.
16. D. Wright, *The amalgamated free product structure of $GL_2(k[X_1, ..., X_n])$ and the weak Jacobian theorem for two variables*, J. Pure Appl. Algebra **12** (1978), 235-251.

Vladimir Shpilrain
Department of Mathematics, University of California, Santa Barbara, CA 93106
*e-mail address*: shpil@math.ucsb.edu

Jie-Tai Yu
Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong
*e-mail address:* yujt@hkuxa.hku.hk