A p-adic approach to the Jacobian Conjecture

Arno van den Essen\textsuperscript{a}\textsuperscript{*} and Richard J. Lipton\textsuperscript{b}

October 16, 2014

\textsuperscript{a} Department of Mathematics, Radboud University Nijmegen, The Netherlands
\textsuperscript{b} Georgia Tech, College of Computing, Atlanta GA 30332, USA

Abstract

It is shown that the Jacobian Conjecture (in all dimensions) is equivalent to the following statement: for almost all prime numbers $p$ and each Keller map $F \in \mathbb{Z}_p[X]^n$ (i.e. $\det JF = 1$), the induced map $\overline{F} : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is not the zero map.

MSC:14R15;13J15

keywords: Jacobian Conjecture, $p$-adic integers

Introduction

The Jacobian Conjecture asserts that every polynomial map $f \in \mathbb{C}[X]^n$ with $\det Jf = 1$ is invertible, i.e. has an inverse map in $\mathbb{C}[X]^n$. Since the formulation of this conjecture in 1939 by Keller ([Ke]), many equivalent formulations of it have been given (see [BCW] or [Es]). The aim of this paper is to give another new, surprising, equivalent description of this conjecture which is based on properties of polynomial maps over the $p$-adic integers.

To describe this result let $F = (F_1, \cdots, F_n)$ be a polynomial map with coefficients in the $p$-adic integers $\mathbb{Z}_p$. By reducing the coefficients of $F$ mod $p\mathbb{Z}_p$ we obtain a polynomial map $\overline{F} : \mathbb{F}_p^n \to \mathbb{F}_p^n$. The main result of this paper states that the Jacobian Conjecture is equivalent to the following statement: if $p$ is a prime number and $F \in \mathbb{Z}_p[X]^n$ a polynomial map with $\det JF = 1$.

\textsuperscript{*}corresponding author: essen@math.ru.nl
then $F$ is not the zero-map. In fact, if the Jacobian Conjecture is true it follows that $F$ is a bijection, namely it follows from [Es], 1.1.12 that the Jacobian Conjecture also holds for polynomial maps with coefficients in $\mathbb{Z}_p$.

So $F$ has an inverse $G$ in $\mathbb{Z}_p[X]^n$. Reducing the equation $F \circ G = X \mod p\mathbb{Z}_p$ we obtain that $F$ is a bijection with inverse $G$.

**Transitivity**

In this section we investigate 2-transitivity of $\text{Aut}_R R^{[n]}$ on $R^n$, where $R$ is a commutative ring, i.e. we investigate under which conditions on $R$ any two points $a \neq b$ of $R^n$ can be send to any two points $c \neq d$ of $R^n$ by an automorphism of $R^{[n]}$.

Let $a, b$ be two different elements of $R^n$ and $c, d$ another such pair. A morphism from $V = \{a, b\}$ to $W = \{c, d\}$ is a polynomial map $F = (f_1, \ldots, f_n) \in R[X]^n$ such that $F(a) = c$ and $F(b) = d$. We say that $V$ and $W$ are isomorphic if there exists a morphism $F$ from $V$ to $W$ and a morphism $G$ from $W$ to $V$ such that $G \circ F = 1_V$ and $F \circ G = 1_W$. Our first aim is to investigate under what conditions two sets $V$ and $W$ are isomorphic. We use the notations as above and introduce one more notation: if $a \in R^n$ we denote by $(a)$ the ideal in $R$ generated by the $a_i$, i.e. $(a) = \sum_i Ra_i$ and if $(a) = R$ then $a$ is called unimodular.

**Proposition 1.**

i) There exists a morphism $V \to W$ if and only if $(d - c) \subseteq (b - a)$.

ii) $V$ and $W$ are isomorphic if and only if $(d - c) = (b - a)$.

**Proof.**

i) $(\Rightarrow)$ Let $F$ be a morphism sending $a$ to $c$ and $b$ to $d$. Then $G := (X - c) \circ F$ is a morphism sending $a$ to $0$ and $b$ to $d - c$. Let $G = (g_1, \ldots, g_n)$. Then $g_i(a) = 0$ implies that $g_i = p_{i1}(X)(X_1 - a_1) + \cdots + p_{in}(X)(X_n - a_n)$, for some $p_{ij}(X)$ in $R[X]$. Since $G(b) = d - c$, we deduce that

$$d_i - c_i = p_{i1}(b)(b_1 - a_1) + \cdots + p_{in}(b)(b_n - a_n), \text{ for all } i$$

$(\Leftarrow)$ Since $(d - c) \subseteq (b - a)$, there exist $p_{ij} \in R$ such that

$$d_i - c_i = p_{i1}(b_1 - a_1) + \cdots + p_{in}(b_n - a_n), \text{ for all } i$$

Let $G = (g_1, \ldots, g_n)$, where $g_i = p_{i1}(X_1 - a_1) + \cdots + p_{in}(X_n - a_n)$. Then $G(a) = 0$ and $G(b) = d - c$. Now put $F = (X + c) \circ G$. Then $F(a) = c$. 

2
and \( F(b) = d \). So \( F \) is a morphism from \( V \) to \( W \). This proves i). Finally ii) follows readily from i).

In the next theorem we assume that \( R \) is a PID. We will show that in case \( V \) and \( W \) are isomorphic, the isomorphism can be extended to an automorphism of \( R^n \), i.e. there exists an \( F \in \text{Aut}_R R^n \) such that \( F(a) = c \) and \( F(b) = d \).

**Theorem 2.** If \( \{a, b\} \) and \( \{c, d\} \) are isomorphic, then there exists an affine automorphism \( f \) of \( R^n \) with \( \det Jf = 1 \) such that \( f(a) = c \) and \( f(b) = d \).

**Proof.** Since \( R \) is a PID, there exists \( g \in R \) such that \( (b - a) = Rg \). Write \( b_i - a_i = gv_i \), for some \( v_i \in R \). Then \( v := (v_1, \ldots, v_n) \) is a unimodular row.

Since \( R \) is a PID this implies that there exists a matrix \( B \in \text{Sl}_n(R) \) which first column equals \( v^t \). Let \( A \) be the inverse of \( B \) and \( (r_{i1}, r_{i2}, \ldots, r_{in}) \) denote the \( i \)-th row of \( A \). Define

\[
F_i := r_{i1}(X_1 - a_1) + \cdots + r_{in}(X_n - a_n), \text{ for all } 1 \leq i \leq n
\]

Then \( F = (F_1, \ldots, F_n) \) satisfies \( F(a) = 0 \). Now we compute \( F(b) \). Let \( 1 \leq i \leq n \). Then

\[
F_i(b) = r_{i1}(b_1 - a_1) + \cdots + r_{in}(b_n - a_n) = g(r_{i1}v_1 + \cdots + r_{in}v_n)
\]

But this element is exactly \( g \) times the product of the \( i \)-th row of \( A \) and the first column of \( B \). Since \( AB = I_n \) this product equals 0 if \( i > 1 \), i.e. \( F_i(b) = 0 \) if \( i > 1 \) and the product equals \( g \) if \( i = 1 \) i.e. \( F_1(b) = g \). Clearly \( F \) is an affine automorphism with \( \det JF = 1 \) sending \( a \) to 0 and \( b \) to \( ge_1 \), where \( e_1 \) is the first unit standard basis vector. Since \( (d - c) = (b - a) = Rg \) we can apply the same argument to find an affine automorphism \( G \) with \( \det JG = 1 \) such that \( G(c) = 0 \) and \( G(d) = ge_1 \). Then one readily verifies that \( f := G^{-1} \circ F \) is an affine automorphism with \( \det Jf = 1 \) such that \( f(a) = c \) and \( f(b) = d \).

The unimodular conjecture

A map \( F \in R[X]^n \) with \( \det JF = 1 \) will be called a Keller map.

**Unimodular Conjecture.** Let \( R \) be a commutative ring contained in a \( \mathbb{Q} \)-algebra. If \( F \) is a Keller map then \( F(b) \) is unimodular for some \( b \in R^n \).

Below the unimodular conjecture will be used as follows:
Proposition 3. Assume that the unimodular conjecture holds for $R$, then for every Keller map $F$ and every $a \in R^n$ there exists $d \in R^n$ such that $F(d) - F(a)$ is unimodular.

Proof. Put $G(X) = F(X + a) - F(a)$. Then $G$ is a Keller map, so by the unimodular conjecture there exists $b \in R^n$ such that $G(b)$ is unimodular, i.e. such that $F(b + a) - F(a)$ is unimodular. Then take $d = b + a$.

Theorem 4. Let $R$ be a PID and assume that the unimodular conjecture holds for $R$. If there exists a Keller map such that $F : R^n \to R^n$ is not injective, then for every $m \geq 2$ there exists a Keller map which has a fiber containing at least $m$ elements.

Proof. i) It suffices to show that if $F$ is a Keller map such that $F(a_1) = \cdots = F(a_m) = c$, where $m \geq 2$ and all $a_i$ are different, then there exists a Keller map $G$ such that $\#G^{-1}(c) \geq m + 1$.

ii) Since $F(a_1) = F(a_2)$ it follows from [CD] or [Es], lemma 10.3.11 ii) that $(a_2 - a_1) = R$. By proposition 3 there exists $d$, such that $(F(d) - F(a_1)) = R$. So $(F(d) - F(a_1)) = (a_2 - a_1)$. By proposition 1, using that $c = F(a_1)$, this means that $\{F(d), c\}$ is isomorphic to $\{a_2, a_1\}$.  By theorem 2 this implies that there exists a Keller map $T$ such that $T(F(d)) = a_2$ and $T(c) = a_1$.

iii) Now put $G = F \circ T \circ F$. Then clearly $G$ is a Keller map. Furthermore

$$G(a_i) = F \circ T(F(a_i)) = F(T(c)) = F(a_i) = c, \text{ for all } 1 \leq i \leq m$$

$$G(d) = F \circ T(F(d)) = F(T(F(d))) = F(a_2) = c$$

Finally observe that $d$ is different from all $a_i$, since $F(a_i) = c$ for each $i$ and $(F(d) - F(a_1)) = R$. So $G^{-1}(c)$ contains at least $m + 1$ elements.

Relations with the Jacobian Conjecture

In this section we show that the Jacobian conjecture is true, if the unimodular conjecture holds for the ring $Z_p$ of $p$-adic integers, for all primes $p$. The proof is based on the following result, which is a special case of a version of Hensel’s lemma ([B], Chap.III. section 4, Corollaire 2):

Theorem (Hensel). Let $F \in Z_p[X]^n$ be a Keller map. If $a \in Z_p^n$ is such that $F(a)$ is in $(pZ_p)^n$, then there exists a unique $b \in Z_p^n$ such that $F(b) = 0$ and $b_i \equiv a_i (mod pZ_p)$ for all $i$. 

4
Theorem 5. If $F \in \mathbb{Z}_p[X]^n$ is a Keller map and $c \in \mathbb{Z}_p^n$ then $\#F^{-1}(c) \leq p^n$.

Proof. If $\#F^{-1}(c) = 0$ we are done, so assume that $\#F^{-1}(c) \geq 1$, say $c = F(a)$ for some $a \in \mathbb{Z}_p^n$. Then $G = F - c$ is a Keller map in $\mathbb{Z}_p[X]^n$ and $F^{-1}(c) = G^{-1}(0)$. If $b \in F^{-1}(c) = G^{-1}(0)$, then $G(b) = 0 \in (p\mathbb{Z}_p)^n$. So by Hensel’s theorem $b$ is completely determined by the element $b \in (\mathbb{Z}_p/p\mathbb{Z}_p)^n$. Since there are at most $p^n$ choices for $b$ (for $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$), there are also at most $p^n$ choices for $b \in G^{-1}(0) = F^{-1}(c)$, which concludes the proof.

Theorem 6. The Jacobian conjecture is true if the unimodular conjecture is true for the $p$-adic integers, for almost all $p$.

Proof. i) It is well-known that it suffices to prove the Jacobian Conjecture for Keller maps with integers coefficients ([Es], 1.1.19). So let $F \in \mathbb{Z}[X]^n$ with $\det JF = 1$. We view $F$ as a map from $\overline{\mathbb{Q}}^n$ to $\overline{\mathbb{Q}}^n$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. It suffices to show that this map is injective, because it then follows that $F$ is invertible over $\overline{\mathbb{Q}}$ ([Es], 4.2.1) and hence, since $\det JF = 1$, $F$ is invertible over $\mathbb{Z}$ ([Es], 1.1.8).

ii) Assume that $F(a) = F(b)$ with $a \neq b \in \overline{\mathbb{Q}}^n$. Then for almost all $p$ we can embed $\mathbb{Z}[a_1, \ldots, a_n, b_1, \ldots, b_n]$ into $\mathbb{Z}_p$ ([Es], 10.3.1). Choose such a $p$ and consider $F : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$. Since $F(a) = F(b)$ with $a \neq b \in \mathbb{Z}_p^n$ and, by assumption, the unimodular conjecture holds for $\mathbb{Z}_p$, it follows from theorem 4 that there exists a Keller map with coefficients in $\mathbb{Z}_p$ which has a fiber of at least $p^n + 1$ elements. This contradicts theorem 5 and completes the proof.

The main result of this paper, theorem 7 below, follows from theorem 6 and the following remark:

Remark. If $R = \mathbb{Z}_p$ the unimodular conjecture is equivalent to: if $F \in \mathbb{Z}_p[X]^n$ is a Keller map, its induced map $\overline{F} : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is not the zero-map.

Proof. Just observe that an element of $u \in \mathbb{R}_p^n$ is unimodular if and only if $\overline{u} \in \mathbb{F}_p^n$ is unimodular (since $\mathbb{Z}_p$ is a local ring) or equivalently if $\overline{u} \neq 0$ in $\mathbb{F}_p^n$.

Theorem 7. The Jacobian Conjecture is equivalent to the following statement: for almost all prime numbers $p$ each Keller map $F \in \mathbb{Z}_p[X]^n$ has the property that its induced map $\overline{F} : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is not the zero-map.

Final remarks on the unimodular conjecture

Proposition 8. The Jacobian Conjecture (over $\mathbb{C}$) implies the unimodular conjecture.
Proof. Let \( F \in R[X]^n \) be a Keller map and \( R \) a ring contained in a \( \mathbb{Q} \)-algebra. Since the Jacobian Conjecture over \( \mathbb{C} \) implies the Jacobian Conjecture over all such rings \( R \) ([Es], 1.1.12), \( F \) has a polynomial inverse over \( R \), say \( G \). Let \( u \) be unimodular. Put \( b = G(u) \). Then \( F(b) = u \), is unimodular.

In order to prove the Jacobian Conjecture we only need the unimodular conjecture to be true for local rings. To conclude this paper we will show that for local rings containing the rationals the unimodular conjecture is true:

**Proposition 9.** Let \( R \) be a local ring with maximal ideal \( m \) such that \( \mathbb{Q} \subseteq R \). Then the unimodular conjecture holds for \( R \).

**Proof.** Let \( F = (F_1, \cdots, F_n) \in R[X]^n \) be a Keller map. As in the proof of the remark above it suffices to show that \( \overline{F} : k^n \to k^n \) is not the zero-map, where \( k = R/m \) is the residue field of \( R \). However this follows easily since the hypothesis \( \mathbb{Q} \subseteq R \) implies that \( \mathbb{Q} \subseteq k \). So \( k \) is an infinite field. If \( \overline{F} : k^k \to k^n \) is the zero-map, this implies that \( \overline{F}_i = 0 \) for each \( i \). So for all \( i \) all coefficients of \( F_i \) belong to the maximal ideal \( m \), contradicting the hypothesis \( \det JF = 1 \).

**References**


