ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 23, Number 1, Winter 1993

ON JACOBIAN n-TUPLES IN CHARACTERISTIC p

JEFFREY LANG AND SATYAGOPAL MANDAL

0. Introduction. Let k be a field and $A = k[x_1, \dots, x_n]$. For $(F_1, \dots, F_n) \in A^n$, let $j(F_1, \dots, F_n)$ denote the determinant of the $n \times n$ Jacobian matrix of $F_1, \dots, F_n$ with respect to the x_i, $1 \le i \le n$. We say that $(F_1, \dots, F_n) \in A^n$ is a *Jacobian n-tuple* if $j(F_1, \dots, F_n) \in k^*$, the multiplicative group of nonzero elements in k. The Jacobian conjecture states:

(0.1) If $\operatorname{char}(k) = 0$, then $j(F_1, \dots, F_n) \in k^*$ implies $k[F_1, \dots, F_n] = A$.

This conjecture, introduced by O.H. Keller [**5**] in 1939, has remained unsolved, for $n \ge 2$, and (0.1) is not true if the characteristic of k is positive ([**1**, p. 118]). Nonetheless, we feel that the study of Jacobian n-tuples when the characteristic is positive may contribute to a better understanding of Jacobian n-tuples in characteristic 0 for two reasons. Firstly, E. Connell and L. van den Dries have shown that the general Jacobian conjecture is equivalent to proving (0.1) for the case where $F_1, \dots, F_n$ are cubic polynomials with integer coefficients (see (1.1) below); thus, information we obtain in characteristic p on cubic Jacobian n-tuples may be related backwards to the characteristic 0 situation. Secondly, S. Abhyankar proved various equivalent formulations of (0.1) in the $n = 2$ case in terms of Newton Polygons, points at infinity, and the degrees of F_1 and F_2 in [**1**] (see (1.3) below). Since for each Jacobian pair in characteristic 0, there are corresponding Jacobian pairs with matching supports in characteristic p for almost all p, our hope is to eventually shed some light on the $n = 2$ case of (0.1) (see (1.2) below).

In this paper we give some new characterizations of Jacobian n-tuples in characteristic p in terms of the differential operator $\nabla =$

Received by the editors on October 1, 1990, and in revised form on April 29, 1991.
Partially supported by the General Research Fund at the University of Kansas.

$\partial^{n(p-1)}/\partial x_1^{p-1} \cdots \partial x_n^{p-1}$; which leads to a method of testing the monomials $F_1^{i_1} \ldots F_n^{i_n}$, one at a time (see (2.1) and (2.2)). The task of relating this new information to Jacobian n-tuples in characteristic 0 is still ahead.

1. Preliminaries.

(1.0.1) We let $\mathbf{Z}$ denote the integers, $\mathbf{Z}^+$ the nonnegative integers, $\mathbf{Q}$ the rationals and $\mathbf{C}$ the complex numbers.

(1.0.2) Let k be a field. k^n denotes the set of n-tuples of elements of k, A_k^n denotes affine n-space over k.

(1.0.3) Let $A = k[x_1, \ldots, x_n]$ be the polynomial ring in n indeterminates over k. Let L be the field of quotients of A.

Given $f \in A$, $\deg_{x_i}(f)$ denotes the degree of f in x_i, $\deg_{x_i, x_j}(f)$ is the degree of f in x_i and x_j, etc.

(1.0.4) For $1 \leq i \leq n$, let $D_i = \partial/\partial x_i$. Given $f_1, \ldots, f_n \in A$, let $J(f_1, \ldots, f_n)$ be the $n \times n$ matrix,

$$\begin{bmatrix} D_1(f_1) & \cdots & D_n(f_1) \\ \vdots & & \vdots \\ D_1(f_n) & \cdots & D_n(f_n) \end{bmatrix},$$

and let $j(f_1, \ldots, f_n)$ be the determinant of $J(f_1, \ldots, f_n)$. $(f_1, \ldots, f_n)$ is called a *Jacobian n-tuple* if $j(f_1, \ldots, f_n)$ is a nonzero element of k.

(1.0.5) θ will denote a generic (i.e., unspecified) nonzero element of k.

(1.0.6) If the characteristic of k is $p \neq 0$, ∇ denotes the differential operator $\nabla = D_1^{p-1} \cdots D_n^{p-1}$.

The following theorem of Connell and van den Dries and our own proposition (1.2) when coupled with Abhyankar's theorem (1.3) suggests that information on Jacobian n-tuples in positive characteristic may be useful via a reduction modulo p approach. In the next section we give some new characterizations of such n-tuples. Assume $F : \mathbf{C}^m \to \mathbf{C}^m$ is a polynomial map defined by $F_1, \dots, F_m \in \mathbf{C}[x_1, \dots, x_m]$. Let T be the ring of algebraic integers. Let $p \subseteq T$ be a nonzero prime ideal and $A = T_p$.

Theorem 1.1 (E. Connell and L. van den Dries). *If there is a counterexample F to the Jacobian conjecture, $F : \mathbf{C}^m \to \mathbf{C}^m$, then for some $n > m$, there is a counterexample $F : \mathbf{C}^n \to \mathbf{C}^n$ where the coefficients of each F_i are in $\mathbf{Z}$ and $F : A^n \to A^n$ is injective. Furthermore, it may be assumed that $F_i = x_1 + u_i$, where $u_i \in \mathbf{Z}^{[n]}$ is a form of degree* 3. ([**4**, Theorem (1.5)]).

Assume now that k is a field and $f = \sum_{i+j=0}^{n} \alpha_{ij} x^i y^j \in k[x, y]$ is a polynomial of degree n. Define $S(f) = \{(i, j) \in \mathbf{Z}^+ \times \mathbf{Z}^+ : i+j \leq n$ and $\alpha_{ij} \neq 0\}$ and $N(f)$ to be the smallest convex subset of $\mathbf{R}^2$ containing $S(f) \cup \{(0, 0)\}$. $S(f)$ is called the *support* of f and $N(f)$ is the *Newton-Polygon* of f. We then have

Proposition 1.2. *Let $f, g \in \mathbf{C}[x, y]$. If $J(f, g) = 1$, then for all but a finite number of prime numbers $p > 0$, there exists a finite field k of characteristic p and a pair of elements $\tilde{f}, \tilde{g} \in k[x, y]$ such that $S(\tilde{f}) = S(f), S(\tilde{g}) = S(g)$ and $j(\tilde{f}, \tilde{g}) = 1$. (Clearly $N(f) = N(\tilde{f})$ and $N(g) = N(\tilde{g})$ as well.)*

Proof. Let $f = \sum \alpha_{ij} x^i y^j$ and $g = \sum \beta_{ij} x^i y^j$ belong to $\mathbf{C}[x, y]$ with $j(f, g) = 1$. If we think temporarily of the α_{ij} and β_{ij} as variables and equate coefficients on both sides of the equality $j(f, g) = 1$, then we obtain a system of equations

(1.2.1) $$F_1 = \cdots = F_r = 0 \quad \text{with } F_1, \dots, F_r \in \mathbf{Z}[\alpha_{ij}, \beta_{ij}].$$

For each $\alpha_{ij} \neq 0$ and $\beta_{i'j'} \neq 0$ the equations $\alpha_{ij} u_{ij} - 1$ and $\beta_{i'j'} v_{i'j'} - 1$ has a solution in $\mathbf{C}$. Let $G_1, \dots, G_s$ be a listing of these equations. Then the G_j's belong to $\mathbf{Z}[\alpha_{ij}, \beta_{ij}, u_{ij}, v_{ij}] = S$. Combine these equations with those of (1.2.1) to obtain a system

(1.2.2)
$$F_1 = \cdots = F_r = G_1 = \cdots = G_s = 0 \quad \text{with the } F\text{'s and } G\text{'s in } S.$$

Since (1.2.2) has a solution in $\mathbf{C}^M$ (M, the number of variables), (1.2.2) has a solution in a finite field of characteristic $p > 0$ for all but a finite number of primes p and such solution will yield a pair $\tilde{f}, \tilde{g}$ with $J(\tilde{f}, \tilde{g}) = 1$ and $S(f) = S(\tilde{f})$, $S(g) = S(\tilde{g})$.

Theorem 1.3 (Abhyankar). *Let k be a field of characteristic* 0*. Then the following statements are equivalent.*

(i) *If $f, g \in k[x, y]$ and $j(f, g) = \theta$, then $k[f, g] = k[x, y]$.*

(ii) *If $f, g \in k[x, y]$ and $j(f, g) = \theta$, then f has one point at infinity.*

(iii) *If $f, g \in k[x, y]$ and $J(f, g) = \theta$, then the Newton-Polygon of f is a triangle with vertices $(n, 0), (0, n)$, and $(0, 0)$ for some nonnegative integers n and m.*

(iv) *If $f, g \in k[x, y]$ and $j(f, g) = \theta$, then* $\deg f$ *divides* $\deg g$ *or* $\deg g$ *divides* $\deg f$. ([**1**, Theorem (19.4)]).

We will also make use of a theorem of P. Samuel. Assume R is a Krull ring of characteristic $p \neq 0$. Let Δ be a derivation on E, the quotient field of R such that $\Delta(R) \subset R$. Let $F = \ker(\Delta)$ and $S = R \cap S$. We have,

Theorem 1.4 (Samuel). (a) *If $[E : F] = p$, then there exists $a \in S$ such that $\Delta^p = a\Delta$,*

(b) *$t \in E$ is equal to $u^{-1}\Delta u$ for some $u \in E$ if and only if* $\Delta^{p-1}t - at + t^p = 0$ ([**7**, Propositions (3.1) and (3.2)]).

2. The Jacobian condition in characteristic p. Assume in this section that the characteristic of k is $p \neq 0$ and that $F_1, \dots, F_n$ are elements of A. For each $i = 1, \dots, n$, let d_i be the k-derivation on L defined by $d_i(h) = j(F_1, \dots, F_{i-1}, h, F_{i+1}, \dots, F_n)$. It is well known that $j(F_1, \dots, F_n) = \theta$ does not imply $A = k[F_1, \dots, F_n]$ ([**1**, p. 118]). The following characterization of Jacobian n-tuples in characteristic p by P. Nousainen appears in [**3**].

Theorem 2.1 (Nousainen). *The following conditions are equivalent.*

(1) $j(F_1, \dots, F_n) = \theta$.

(2) $A = k[x_1^p, \dots, x_n^p, F_1, \dots, F_n]$.

(3) *The monomials* $F_1^{q_1} \cdots F_n^{q_n}$, $0 \le q_i \le p-1$, *form a free basis of the* $k[x_1^p, \dots, x_n^p]$*-module* A. ([**3**, Theorem (2.2)]).

Our main result extends Nousainen's theorem and gives us a way to test the monomials $F_1^{q_1} \cdots F_n^{q_n}$ individually.

Theorem 2.2. *The following are equivalent.*

(1) $j(F_1, \dots, F_n) = \theta$.

(4) *For each* $i = 1, \dots, n$, *and each* $h \in L$, $h = \theta \sum_{r=0}^{p-1} F_i^r d_i^{p-1} \cdot (F_i^{p-r-1} h)$.

(5) $\nabla = \theta d_1^{p-1} \cdots d_n^{p-1}$

(6) $$\nabla(F_1^{q_1} \cdots F_n^{q_n}) = \begin{cases} 0, & \text{if } 0 \le q_i < p-1, \text{ for some } i = 1, \dots, n. \\ \theta, & \text{if } q_1 = \cdots = q_n = p-1. \end{cases}$$

Lemma 2.3. *Let* R *be Krull ring of characteristic* $p \neq 0$ *with quotient field* F *and* $D\colon F \to F$ *a derivation. Let* $F' = D^{-1}(0)$. *Assume* $D(R) \subset R$, $[F : F'] = p, R' = F' \cap R$ *and* $f \in R$. *Then* $D(f) \in \mathbf{F}_p^*$, *the multiplicative group of nonzero elements of the prime subfield of* R, *if and only if* $Df \in R'$ *and for all* $a \in R$, $a = -\sum_{i=0}^{p-1} f^{p-i-1} D^{p-1}(f^i a)$.

Proof. ($\Rightarrow$). Assume $Df = b \in F_p^*$. Then $0 = D(1) = D(b^{p-1}) = -b^{p-2} Db$, which shows that $D(b) = 0$. By (1.4), $D^p = \alpha D$ for some $\alpha \in R'$. Then $D^p f = \alpha Df$ implies $\alpha = 0$. Therefore, $D^{p-1} c \in R'$ for all $c \in R$.

Let $a \in R$. Let $\beta = \sum_{i=0}^{p-1} f^{p-i-1} D^{p-1}(f^i a)$. Then

$$\begin{aligned} \beta &= \sum_{i=0}^{p-1} f^{p-i-1} \sum_{j=0}^{p-1} \binom{p-1}{j} D^j(f^i) D^{p-1-j}(a) \\ &= \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} (-1)^j \binom{i}{j} (j!) b^j f^{p-1-j} D^{p-1-j}(a) \\ &= \sum_{j=0}^{p-1} \sum_{i=0}^{p-1} (-1)^j \binom{i}{j} (j!) b^j f^{p-1-j} D^{p-1-j}(a). \end{aligned}$$

(We are following the convention that $\binom{i}{j} = 0$ if $j > i$.)

$$\begin{aligned}\beta &= \sum_{j=0}^{p-1}(-1)^j(j!)b^j f^{p-1-j}D^{p-1-j}(a)\sum_{i=0}^{p-1}\binom{i}{j}\\ &= \sum_{j=0}^{p-1}(-1)^j(j!)b^j f^{p-1-j}D^{p-1-j}(a)\binom{p}{j+1}.\end{aligned}$$

Since $\operatorname{char}(A) = p$, $\binom{p}{j+1} = 0$ unless $j = p-1$. Therefore, $\beta = (-1)^{p-1}(p-1)!b^{p-1}f^0D^0(a) = -a$.

($\Leftarrow$). If $a = -\sum_{i=0}^{p-1} f^{p-i-1}D^{p-1}(f^i a)$ for all $a \in A$, then in particular, $1 = -\sum_{i=0}^{p-1} f^{p-i-1}D^{p-1}(f^i)$. Since $Df \in R'$ we obtain $1 = -(p-1)!(Df)^{p-1}$. Therefore, $(Df)^{p-1} = 1$ and $Df \in \mathbf{F}_p^*$. □

Lemma 2.4. *Let R, R', D, and f be as in (2.3). If $Df \in R^*$, the group of units in R, then $R = R'[f]$.*

Proof. Let $\Delta = (Df)^{-1}D$. By (2.3), we have for all $a \in R$, $a = -\sum_{i=0}^{p-1} f^{p-i-1}\Delta^{p-1}(f^i a)$. By (1.4), there exists an $\alpha \in R'$ such that $\Delta^p = \alpha\Delta$. Since $\Delta f = 1$, $\alpha = 0$. Thus, $\Delta^{p-1}(a) \in R'$ for all $a \in R$. □

Lemma 2.5. *Let R, R', D, and f be as in (2.3). Assume that the ideal $D(R)\cdot R$ is not contained in any height one prime and $Df \neq 0$. Then the following are equivalent.*

(1) *$Df \in (R')^*$, the multiplicative group of units in R'.*

(2) *$Df \in R'$* and *$R'[f] = R$.*

(3) *$Df \in R'$ and there exists $\beta \in (R')^*$ such that for all $a \in R$,*

$$a = \beta\sum_{i=0}^{p-1} f^{p-i-1}D^{p-1}(f^i a).$$

Proof. (1) $\Rightarrow$ (3) $\Rightarrow$ (2): Repeat the proof of (2.4) noting by (1) that $Df \in R'$. (2) $\Rightarrow$ (1): $Df \in R'$ and $R'[f] = R$ implies that

$D(R) \subseteq (Df) \cdot R$. Since $D(R)R$ is not contained in any height one prime of R, $Df \in R^* \cap R' = (R')^*$. □

(2.6). Assume that k is algebraically closed. Let $A' = A^p[F_1, \dots, F_{n-1}]$ and $L' = L^p[F_1, \dots, F_n]$ be the quotient field of A'. Let I be the ideal in A generated by the $n-1 \times n-1$ minors of the matrix

$$\begin{bmatrix} D_1(F_1) & \cdots & D_n(F_1) \\ \vdots & & \vdots \\ D_1(F_{n-1}) & \cdots & D_n(F_{n-1}) \end{bmatrix}.$$

That is, I is generated by $d_n(x_i)$, $1 \le i \le n$. We say that $F_1, \dots, F_{n-1}$ satisfy condition $(*)$ if the dimension of A/I is at most $n-2$.

Lemma 2.7. *Let $X \subseteq A_k^{2n-1}$ be the variety defined by the equations $y_i^p = F_i$, $1 \le i \le n-1$. If the F_i satisfy $(*)$, then the coordinate ring of X is isomorphic to A'.*

Proof. Let $\phi : A \to A'$ be the ring homomorphism that sends x_i to x_i^p, w_j to F_j and α to α^p for all $1 \le i \le n$, $1 \le j \le n-1$, $\alpha \in k$. (Note that ϕ is not a k-homomorphism.) Then $\omega_j^p - F_j \in \ker \phi$. Let $Q \subseteq A$ be the ideal generated by $w_j^p - F_j$, $1 \le j \le n-1$. By (*) $F_1 \notin A^p$ and $F_j \notin A^p[F_1, \dots, F_{j-1}]$, $2 \le j \le n-1$. It follows that Q is a prime ideal of height $n-1$. Therefore, $\ker \phi = Q$. □

Lemma 2.8. *If the F_i satisfy $(*)$, then $A \cap d_n^{-1}(0) = A'$.*

Proof. Let $B = d_n^{-1}(0) \cap A$. Then $A^p \subseteq A' \subseteq B \subseteq A$. By $(*)$, each $F_j \notin L^p(F_1, \dots, F_{j-1})$. Thus, $[L' : L^p] = p^{n-1}$. Also, by $(*)$, $d_n(x_i) \neq 0$ for some i. Therefore, the quotient field of B is not L and hence A' and B have the same quotient field. Clearly, B is integral over A'. By (2.7), A' is isomorphic to the coordinate ring of X, which is regular in codimension one by $(*)$. Therefore, A' is normal, which proves $A' = B$. □

The proof of the next lemma appears in [**6**].

Lemma 2.9. *Without the assumption of* $(*)$,

(1) *there exists* $\beta \in A'$ *such that* $d_n^p = \beta d_n$. β *is given by the formula*

$$\beta = (-1)^n \sum_{j=1}^{n-1} \sum_{r_j=0}^{p-1} F_1^{r_1} \cdots F_{n-1}^{r_{n-1}} \nabla(F_1^{p-r_1-1} \cdots F_{n-1}^{p-r_{n-1}-1});$$

(2) *furthermore, for all* $t \in L$,

$$d_n^{p-1}(t) - \beta t = (-1)^{n-1} \sum_{j=1}^{n-1} \sum_{r_j=0}^{p-1} F_1^{r_1} \cdots F_{n-1}^{r_{n-1}} \nabla(F_1^{p-r_1-1} \cdots F_{n-1}^{p-r_{n-1}-1} t).$$

Proof of Theorem (2.2). (1) $\Rightarrow$ (4): (1) is true up to a permutation of the F_i; thus, it is enough to prove (4) for $i = n$. (1) implies $(*)$. Now use (3) of (2.5).

(4) $\Rightarrow$ (5): For all $h \in L$, $h = \theta \sum_{r=0}^{p-1} F_n^r (d_n^{p-1}(F_n^{p-r-1} h) - \beta F_n^{p-r-1} h)$, where $d_n^p = \beta d_n$, since $\sum_{r=0}^{p-1} \beta F_n^{p-1} h = 0$. By (2.9), we see that for all $h \in L$,

$$\text{(A)} \qquad h = \theta \sum_{j=1}^{n} \sum_{r_j=0}^{p-1} F_1^{r_1} \cdots F_n^{r_n} \nabla(F_1^{p-r_n-1} \cdots F_n^{p-r_n-1} h).$$

(A) implies (2) of (2.1), hence (1). By (1), $d_i(F_i) = \theta$, $1 \leq i \leq n$. Apply $d_1^{p-1} \cdots d_n^{p-1}$ to both sides of (A) and use the fact that

$$d_i(F_j) = \begin{cases} 0, & \text{if } i \neq j, \\ \theta, & \text{if } i = j, \end{cases}$$

and $\nabla(A) \subseteq A^p$ to obtain (5).

(5) $\Rightarrow$ (1): Assume $\nabla = d_1^{p-1} \cdots d_n^{p-1}$. Let $g = d_1^{p-2} d_2^{p-1} \cdots d_n^{p-1}(x_1^{p-1} \cdots x_n^{p-1})$. Then $d_1(g) = (-1)^n$. Therefore, $d_1^p = 0$ and by (2) of (2.1), $A = A^p[F_2, \ldots, F_n, g]$. Thus, $[L : L_0] = p$, where $L_0 = L^p(F_2, \ldots, F_n)$. If $F_1 \in L_0$, then $d_n(F_n) = \pm d_1(F_1) = 0$. Then for all $r, i_1, \ldots, i_n \in \mathbf{F}_p$, we have $\nabla(F_n^r x_1^{i_1} \cdots x_n^{i_n}) = \theta d_1^{p-1} \cdots d_n^{p-1}(F_n^r x_1^{i_1} \cdots x_n^{i_n}) = \theta F_n^r d_1^{p-1} \cdots d_n^{p-1}(x_1^{i_1} \cdots x_n^{i_n}) = \theta F_n^r \nabla(x_1^{i_1} \cdots x_n^{i_n})$. Therefore, $\nabla(F_n^r x_1^{i_1} \cdots x_n^{i_n}) =$

0 for all r and $(i_1, \ldots, i_n) \neq (p-1, \ldots, p-1)$. When $r = 1$, this gives $F_n \in A^p$. Then $d_i \equiv 0$, $1 \leq i \leq n-1$, which is a contradiction. Therefore, $F_1 \notin L_0$ and hence $L = L^p(F_1, \ldots, F_n)$. This shows that the d_i, $1 \leq i \leq n$, commute on L, so that for any permutation $\phi \in S_n$, $d_{\phi(1)}^{p-1} \cdots d_{\phi(n)}^{p-1} = \theta\nabla$. Then by the same argument we used for d_1, we get $d_i^p \equiv 0$, $1 \leq i \leq n$. By commutivity, $d_2(g) = 0$. By (2.8), $g \in A^p[F_1, \ldots, F_{n-1}]$. Therefore, $A = A^p[F_2, \ldots, F_n, g] \subseteq A^p[F_1, \ldots, F_n] \subseteq A$, which by (2.1) implies (1). The equivalence of (1) and (6) is a simple corollary to the equivalence of (1) and (5). □

REFERENCES

1. S.S. Abhyankar, *Expansion techniques in algebraic geometry*, Tata Lecture Notes, 1977.

2. ———, *Lectures in algebraic geometry*, Notes by Chris Christiansen, Purdue Univ., 1974.

3. 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.

4. E. Connell and L. van den Dries, *Injective polynomial maps and the Jacobian conjecture*, J. Pure Appl. Algebra **28** (1983), 235–239.

5. O.H. Keller, *Ganze Cremona-Transformationen*, Monatsh Math. **47** (1939), 299–306.

6. J. Lang, *Purely inseparable extensions of unique factorization domains*, Kyoto Journal **26** (1990), 453–471.

7. P. Samuel, *Lectures on unique factorization domains*, Tata Lecture Notes, Bombay, 1964.

Department of Mathematics, University of Kansas, Lawrence, KS, 66045