Hiroshima Math. J.
35 (2005), 351–370

Positive characteristic approach to Weak Kernel Conjecture

Shun-ichi Kimura and Shun-ichiro Okuda

(Received February 17, 2004)
(Revised October 12, 2004)

Abstract. When the polynomials $f_1, \dots, f_n \in \mathbf{C}[x_1, \dots, x_n]$ satisfy the Jacobian condition $\det\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j} \in \mathbf{C}^*$, the Kernel Conjecture says that $\mathrm{Ker}\left(\frac{\partial}{\partial f_n}\right)$ should be $\mathbf{C}[f_1, \dots, f_{n-1}]$. In this paper, we prove a weaker version: When the leading monomials $\mathrm{LM}(f_1), \dots, \mathrm{LM}(f_t)$ of $f_1, \dots, f_t$ (under a given monomial ordering) are linearly independent, then $\bigcap_{i>t} \mathrm{Ker}\left(\frac{\partial}{\partial f_i}\right) = \mathbf{C}[f_1, \dots, f_t]$.

The main tool is the higher derivations $\partial_{f_i}^{[L]}$, which behave like $\frac{1}{L!}\left(\frac{\partial}{\partial f_i}\right)^L$, but are defined for any rings, including positive characteristic ones. We reduce the problem of calculating the (higher) derivation kernels to the positive characteristic case, where we have a better control.

1. Introduction

The celebrated Jacobian Conjecture states that when a polynomial map $\varphi : \mathbf{C}^n \to \mathbf{C}^n$ is locally isomorphic (or étale, in algebraic geometric term), then φ is isomorphic. Algebraically, it says that when the polynomials $f_1, \dots, f_n \in \mathbf{C}[x_1, \dots, x_n]$ satisfy the Jacobian condition, namely when $\det\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j=1,\dots,n}$ is invertible, then $\mathbf{C}[f_1, \dots, f_n] = \mathbf{C}[x_1, \dots, x_n]$, namely these polynomials generate the whole polynomial ring. It is crucial to assume φ to be a polynomial map. The function e^x is an immediate counterexample in 1 variable, and even when we require $\det\left(\frac{\partial f_i}{\partial x_j}\right)$ to be a constant, $(x, y) \mapsto (-e^{-x}, ye^x)$ has Jacobian determinant 1 without being isomorphic.

The Jacobian Conjecture is also false when the characteristic is positive. When k is a field of characteristic $p > 0$, the function $x^p + x \in k[x]$ satisfies the Jacobian condition as $\frac{d}{dx}(x^p + x) = 1$, however $k[x^p + x] \neq k[x]$ ($k(x^p + x) \subset k(x)$ is a field extension of degree p). Still there are several attempts to attack the Jacobian Conjecture via positive characteristic. For example, Adjamagbo [1] conjectures that if the degree of the field extension is not divisible by p, then étale morphisms are isomorphic, which conjecture would imply the Jacobian conjecture in characteristic 0. In this paper, we will make an another attempt via positive characteristic.

2000 *Mathematics Subject Classification*. 13N15, 14R15.
Key words and phrases. Jacobian Conjecture, derivation kernel, SAGBI basis.

In preparation for explaining our approach, we would like to introduce the Kernel conjecture. Let $f_1, \dots, f_n \in k[x_1, \dots, x_n]$ and $g \in k[f_1, \dots, f_n]$ be polynomials. Then one can compute the partial derivative of g by the chain rule; $\frac{\partial g}{\partial x_i} = \sum_{j=1}^{n} \frac{\partial f_j}{\partial x_i} \frac{\partial g}{\partial f_j}$, which can be displayed by matrix form:

$$\begin{pmatrix} \dfrac{\partial g}{\partial x_1} \\ \vdots \\ \dfrac{\partial g}{\partial x_n} \end{pmatrix} = \begin{pmatrix} \dfrac{\partial f_1}{\partial x_1} & \cdots & \dfrac{\partial f_n}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial f_1}{\partial x_n} & \cdots & \dfrac{\partial f_n}{\partial x_n} \end{pmatrix} \begin{pmatrix} \dfrac{\partial g}{\partial f_1} \\ \vdots \\ \dfrac{\partial g}{\partial f_n} \end{pmatrix}$$

Now assume that $f_1, \dots, f_n$ satisfy the Jacobian condition, namely the matrix above is invertible. Then multiplying the inverse matrix from the left, we obtain the formula for $\frac{\partial g}{\partial f_j}$ in terms of $\frac{\partial g}{\partial x_i}$ and $\frac{\partial f_j}{\partial x_i}$, which makes sense even for $g \in k[x_1, \dots, x_n]$, not assuming that $g \in k[f_1, \dots, f_n]$, and we adopt this as the definition of $\frac{\partial}{\partial f_i} : k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]$ (see Definition 2.3). Then the Kernel conjecture states that if $f_1, \dots, f_n$ satisfy the Jacobian condition, then $\mathrm{Ker}\, \frac{\partial}{\partial f_n} = k[f_1, \dots, f_{n-1}]$. The Kernel conjecture for $n+1$ variables implies the Jacobian Conjecture for n variables: When $f_1, \dots, f_n \in k[x_1, \dots, x_n]$ satisfy the Jacobian condition, then $f_1, \dots, f_n, f_{n+1} \in k[x_1, \dots, x_{n+1}]$ with $f_{n+1} = x_{n+1}$ also satisfy the Jacobian condition, and the Kernel conjecture says $k[f_1, \dots, f_n] = \mathrm{Ker}\, \frac{\partial}{\partial f_{n+1}} = k[x_1, \dots, x_n]$. On the other way, suppose the Jacobian Conjecture for n variables. When $f_1, \dots, f_n$ satisfy the Jacobian condition, the polynomials f_i's are just another variables to generate the polynomial ring, and hence the Kernel conjecture for n variables holds. In this sense, the Kernel conjecture is equivalent to the Jacobian Conjecture.

The argument above indicates that the Kernel conjecture is also false for positive characteristics. Interestingly, in positive characteristic, Nousiainen's theorem ([2, Thm 2.2]) is known (see Proposition 2.4), which gives a precise formula for the derivation kernel in characteristic p, namely, $\mathrm{Ker}\, \frac{\partial}{\partial f_n} = k[x_1^p, x_2^p, \dots, x_n^p, f_1, \dots, f_{n-1}]$, when f_i's satisfy the Jacobian condition. In this paper, we start from Nousiainen's theorem, and investigate the behavior of higher derivations. The main technical achievement of this paper is the construction of higher derivations $\partial_{f_i}^{[L]}$ which behave like $\frac{1}{L!}\left(\frac{\partial}{\partial f_i}\right)^L$ for polynomials $f_1, \dots, f_n$ satisfying the Jacobian condition (see Theorem 2.13), then we can give a precise formula for the kernels of these higher derivations. More concretely, we have

$$\bigcap\nolimits_{L>0} \mathrm{Ker}\, \partial_{f_n}^{[L]} = \bigcap\nolimits_{r>0} k[x_1^{p^r}, \dots, x_n^{p^r}, f_1, \dots, f_{n-1}],$$

where the left hand side correspondes to $\mathrm{Ker}\, \frac{\partial}{\partial f_n}$ in characteristic 0.

Recall that in characteristic 0, the calculations of the derivation kernels are much harder. Sometimes, the derivation kernels are not finitely generated as k-algebras [4], and we do not know how to describe the kernel ring. On the other hand in positive characteristic, we even have a concrete algorithm to compute the derivation kernel (see [7] for example). In our case, we do not know if the right hand side of the formula above is finitely generated or not as k-algebra either, but at least we have a precise description.

Good news is that under some condition (admittingly a strong condition), we can prove that the right hand side $\bigcap_{r>0} k[x_1^{p^r}, \dots, x_n^{p^r}, f_1, \dots, f_{n-1}]$ equals $k[f_1, \dots, f_{n-1}]$ (Corollary 4.7). Using the Groebner basis and mimicking the technique of reduction to positive characteristic, used in Mori program, we can lift the results to the characteristic 0 situation.

Bad news is that our condition is too strong to be very useful. So we introduce a Weak Kernel Conjecture 5.1, for which conjecture, we can prove a special case. Our main result states that if $f_1, \dots, f_n$ satisfy the Jacobian condition, and if the leading monomials $LM(f_1), \dots, LM(f_t)$, considered as vectors in $\mathbf{Z}^n \subset \mathbf{Q}^n$, are linearly independent, then $\bigcap_{i>t} \operatorname{Ker} \frac{\partial}{\partial f_i} = k[f_1, \dots, f_t]$ holds (Theorem 5.3). In particular, the Weak Kernel conjecture holds when $t = 1$. It includes the Kernel Conjecture for 2 variables (Corollary 5.4, which is classically known by a different proof, see [6]).

In our approach to Jacobian conjecture, the only missing point is the study of the ring $\bigcap_{r>0} k[x_1^{p^r}, \dots, x_n^{p^r}, f_1, \dots, f_t]$. If one can find a good condition for a k subalgebra $R \subset k[x_1, \dots, x_n]$, in order that the equality $R = \bigcap_{r>0} R[x_1^{p^r}, \dots, x_n^{p^r}]$ holds, then that would imply the Jacobian Conjecture. We have an example $\bigcap_{r>0} k[x^{p^r}, x^p + x] = k[x] \supset k[x^p + x]$, so we need some assumption. It seems (or at least we hope) that if the characteristic of k is "large enough" compared to the multi-degrees of the terms of the generators of R, then the equality holds.

Our construction of higher derivations $\partial_{f_i}^{[L]}$ is based on positive characteristic argument. Let $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition with R a ring with characteristic p^e, a power of a prime, then by Nousiainen's theorem, any polynomial $g \in R[x_1, \dots, x_n]$ can be uniquely written as

$$g = \sum_{0 \le \alpha_1, \dots, \alpha_n < p^N} a_{\alpha_1, \dots, \alpha_n}(x_1^{p^N}, \dots, x_n^{p^N}) f_1^{\alpha_1} \dots f_n^{\alpha_n}$$

for any N (Corollary 2.6). The higher derivaiton $\partial_{f_i}^{[L]}$ should look like $\frac{1}{L!}\left(\frac{\partial}{\partial f_i}\right)^L$, so it is natural to define

$$\partial_{f_i}^{[L]} g = \sum_{0 \le \alpha_1, \dots, \alpha_n < p^N} a_{\alpha_1, \dots, \alpha_n}(x_1^{p^N}, \dots, x_n^{p^N}) \binom{\alpha_i}{L} f_1^{\alpha_1} \dots f_i^{\alpha_i - L} \dots f_n^{\alpha_n}$$

when N is large enough, because any (higher) derivation of $a(x_1^{p^N}, \dots, x_n^{p^N})$ is a multiple of a high power of p, hence is 0 in R coefficient.

We prove that this definition is well defined independent of the choice of N (Proposition 3.6). Hence it induces a definition of a higher derivation in $\varprojlim_e R/(p^e R)[x_1, \dots, x_n]$ when R is Noether (Proposition 3.8). This again induces a higher derivation in $R[x_1, \dots, x_n]$ via the canonical map $R[x_1, \dots, x_n] \to \prod_p \varprojlim_e R/(p^e R)[x_1, \dots, x_n]$ when R is a finitely generated ring over $\mathbf{Z}$ (Proposition 3.12). Finally it induces higher derivations for any ring (Theorem 2.13), because any ring is an inductive limit of finitely generated rings over $\mathbf{Z}$.

2. Nousiainen's Theorem

DEFINITION 2.1. If the unit 1 of a ring R has a finite order N in the additive group, we say that R has *characteristic* N. If the order of 1 is infinite, we say that R has *characteristic* 0.

DEFINITION 2.2. Let R be a ring. Polynomials $f_1, f_2, \dots, f_n \in R[x_1, x_2, \dots, x_n]$ are said to satisfy *the Jacobian condition* when the determinant of the matrix $\left(\frac{\partial f_i}{\partial x_j}\right)_{1 \le i, j \le n}$ is in the multiplicative group of units $R[x_1, \dots, x_n]^*$.

DEFINITION 2.3. Let the polynomials $f_1, f_2, \dots, f_n \in R[x_1, x_2, \dots, x_n]$ satisfy the Jacobian condition. Define a derivation $\frac{\partial}{\partial f_i} : R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ by

$$\begin{pmatrix} \dfrac{\partial}{\partial f_1} \\ \vdots \\ \dfrac{\partial}{\partial f_n} \end{pmatrix} := \begin{pmatrix} \dfrac{\partial f_1}{\partial x_1} & \cdots & \dfrac{\partial f_n}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial f_1}{\partial x_n} & \cdots & \dfrac{\partial f_n}{\partial x_n} \end{pmatrix}^{-1} \begin{pmatrix} \dfrac{\partial}{\partial x_1} \\ \vdots \\ \dfrac{\partial}{\partial x_n} \end{pmatrix}.$$

PROPOSITION 2.4. *Assume that the characteristic of R is a prime number $p > 0$. For polynomials $f_1, f_2, \dots, f_n \in R[x_1, x_2, \dots, x_n]$, the following are equivalent:*

(1) *The polynomials $f_1, f_2, \dots, f_n$ satisfy the Jacobian condition.*

(2) $R[x_1^p, x_2^p, \dots, x_n^p, f_1, f_2, \dots, f_n] = R[x_1, x_2, \dots, x_n]$.

(3) *$R[x_1, x_2, \dots, x_n]$ is a free module over $R[x_1^p, x_2^p, \dots, x_n^p]$ with a basis $\{f_1^{\alpha_1} f_2^{\alpha_2} \cdots f_n^{\alpha_n}\}_{0 \le \alpha_1, \alpha_2, \dots, \alpha_n < p}$.*

PROOF. The implication (3) $\Rightarrow$ (2) is trivial.

For (2) $\Rightarrow$ (1), assuming (2), each x_i can be written as $x_i = \sum a_{i,\alpha}(x_1^p, \dots, x_n^p) f^\alpha$, where $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbf{Z}_{\ge 0}^n$ is a multi-index. Take the partial derivative of both sides by x_j. Then we obtain

$$\delta_{i,j} = \sum a_{i,\alpha}(x_1^p, \ldots, x_n^p)\alpha_\ell f^{\alpha - e_\ell}\frac{\partial f_\ell}{\partial x_j}$$

where $e_\ell = (0,0,\ldots,0,1,0,\ldots,0)$ is a multi-index with the ℓ-th component being 1 and the other components 0. Hence, the matrix $(\sum a_{i,\alpha}(x_1^p,\ldots,x_n^p)\alpha_j f^{\alpha-e_j})_{1\le i,j\le n}$ is the inverse matrix of the Jacobian matrix, which implies (1).

For (1) $\Rightarrow$ (3), we define an $R[x_1^p, x_2^p, \ldots, x_n^p]$-module homomorphism $\varphi : R[x_1, x_2, \ldots, x_n] \to R[x_1, x_2, \ldots, x_n]$ to be

$$\sum_{0\le\alpha_1,\ldots,\alpha_n<p} x_1^{\alpha_1}\ldots x_n^{\alpha_n}\prod_{i=1}^n\left(1 - \left(f_i\frac{\partial}{\partial f_i}\right)^{p-1}\right)\cdot\prod_{i=1}^n\frac{1}{(\alpha_i)!}\left(\frac{\partial}{\partial f_i}\right)^{\alpha_i}.$$

One easily checks that

$$\varphi\left(\sum_{0\le\alpha_1,\ldots,\alpha_n<p} a_\alpha(x_1^p,\ldots,x_n^p)f^\alpha\right) = \sum_{0\le\alpha_1,\ldots,\alpha_n<p} a_\alpha(x_1^p,\ldots,x_n^p)x^\alpha.$$

Letting M be the submodule of $R[x_1,\ldots,x_n]$ generated by the set $\{f_1^{\alpha_1}f_2^{\alpha_2}\ldots f_n^{\alpha_n}\}_{0\le\alpha_1,\alpha_2,\ldots,\alpha_n<p}$, one verifies that φ induces a surjection from M to $R[x_1,\ldots,x_n]$. Because $R[x_1,\ldots,x_n]$ is a free $R[x_1^p,\ldots,x_n^p]$-module with the number of generators exactly same as the generators of M, we conclude that M is freely generated by our generators, and φ is a bijection from M to $R[x_1,\ldots,x_n]$. Hence $R[x_1,\ldots,x_n]$ is a direct sum of M and $\operatorname{Ker}\varphi$, and because $\operatorname{rank} M = \operatorname{rank} R[x_1,\ldots,x_n]$ as $R[x_1^p,\ldots,x_n^p]$-modules, we see that $\operatorname{Ker}\varphi = 0$, proving (3). □

Corollary 2.5. *If $f_1,\ldots,f_n \in R[x_1,\ldots,x_n]$ satisfy the Jacobian condition and R has a prime characteristic p, then* $\left(\frac{\partial}{\partial f_i}\right)^p = 0$.

Proof. Proposition 2.4 implies that when we assume the Jacobian conditoin, any polynomial $g \in R[x_1,\ldots,x_n]$ is written as $\sum a(x_1^p,\ldots,x_n^p)f^\alpha$. The homomorphism $\left(\frac{\partial}{\partial f_i}\right)^p$ is an $R[x_1^p,\ldots,x_n^p]$-homomorphism, so we have only to prove that $\left(\frac{\partial}{\partial f_i}\right)^p f^\alpha = 0$. $\left(\frac{\partial}{\partial f_i}\right)^p f^\alpha$ is $\alpha_i(\alpha_i - 1)\ldots(\alpha_i - p + 1)f^{\alpha - pe_i}$, and one of $\alpha_i, (\alpha_i - 1), \ldots, (\alpha_i - p + 1)$ is a multiple of p, hence it is 0. □

Corollary 2.6. *Suppose R has a characteristic p^e, a power of a prime number p. If $f_1,\ldots,f_n \in R[x_1,\ldots,x_n]$ satisfy the Jacobian condition, then for any positive integer r, we have $R[x_1,\ldots,x_n] = R[x_1^{p^r},\ldots,x_n^{p^r}, f_1,\ldots,f_n]$. Moreover, any polynomial $g \in R[x_1,\ldots,x_n]$ can be uniquely written as*

$$g = \sum_{0\le\alpha_1,\ldots,\alpha_n<p^r} a_\alpha(x_1^{p^r},\ldots,x_n^{p^r})f^\alpha.$$

Proof. First, we assume that $e=1$. For the equality $R[x_1,\dots,x_n]=R[x_1^{p^r},\dots,x_n^{p^r},f_1,\dots,f_n]$, we need to show that $x_i^p\in R[x_1^{p^r},\dots,x_n^{p^r},f_1,\dots,f_n]$ for each i. We proceed by induction on r. The case $r=1$ is done in Proposition 2.4. By the induction hypothesis, we can write $x_i=\sum a_\alpha(x_1^{p^{r-1}},\dots,x_n^{p^{r-1}})f^\alpha$. Applying the Frobenius map, we have

$$x_i^p=\sum\overline{a_\alpha}(x_1^{p^r},\dots,x_n^{p^r})(f^p)^\alpha\in R[x_1^{p^r},\dots,x_n^{p^r},f_1,\dots,f_n],$$

where $\overline{a_\alpha}$ is the polynomial a_α with each coefficient raised to the p-th power.

For each expression $g=\sum a_\alpha(x_1^{p^r},\dots,x_n^{p^r})f^\alpha$, using the fact that $f_i^{p^r}\in R[x_1^{p^r},\dots,x_n^{p^r}]$, we can move $f_i^{p^r}$ to $a_\alpha(x_1^{p^r},\dots,x_n^{p^r})$ until we get $\alpha_i<p^r$ for all α and i.

When $e>1$, let $M\subset R[x_1,\dots,x_n]$ be an $R[x_1^{p^r},\dots,x_n^{p^r}]$ module generated by $\{f_1^{\alpha_1},\dots,f_n^{\alpha_n}\,|\,0\le\alpha_1,\dots,\alpha_n<p^r\}$. Then the $e=1$ case implies that $M+pR[x_1,\dots,x_n]=R[x_1,\dots,x_n]$, hence Nakayama's lemma implies $M=R[x_1,\dots,x_n]$. In particular, we have $R[x_1,\dots,x_n]=R[x_1^{p^r},\dots,x_n^{p^r},f_1,\dots,f_n]$, and each polynomial $g\in R[x_1,\dots,x_n]$ has an expression $g=\sum_{0\le\alpha_1,\dots,\alpha_n<p^r}a_\alpha(x_1^{p^r},\dots,x_n^{p^r})f^\alpha$.

To prove the uniqueness of the expression, observing that the number of generators of M is p^{nr}, which is same as the rank of free module $R[x_1,\dots,x_n]$ as an $R[x_1^{p^r},\dots,x_n^{p^r}]$ module, we can conclude that $\{f_1^{\alpha_1},\dots,f_n^{\alpha_n}\,|\,0\le\alpha_1,\dots,\alpha_n<p^r\}$ is a free basis. □

Lemma 2.7. *Let p be a prime number, R a ring, and assume that $f_1,\dots,f_n\in R[x_1,\dots,x_n]$ satisfy the Jacobian condition. For any positive integer N and M and any polynomial $G\in R[x_1,\dots,x_n]$, there exists a polynomial $a_\alpha(x_1^{p^N},\dots,x_n^{p^N})\in R[x_1^{p^N},\dots,x_n^{p^N}]$ for each multi index α with $0\le\alpha_1,\dots,\alpha_n<p^N$ such that*

$$G-\sum_{0\le\alpha_1,\dots,\alpha_n<p^N}a_\alpha(x_1^{p^N},\dots,x_n^{p^N})f^\alpha\in p^MR[x_1,\dots,x_n].$$

Proof. If $p\in R$ is a unit, the statement is trivial. Otherwise, apply Corollary 2.6 to $(R/p^MR)[x_1,\dots,x_n]$. □

Definition 2.8. When L is a positive integer and p a prime number, define $d_p(L)$ to be the order of multiples of p in $L!$ (namely, $d_p(L)=\mathrm{ord}_p(L!)$ in the usual notation). More concreterly, when $L=\sum_{i=0}^t c_ip^i$, $0\le c_i<p$ is the p-adic representation of L, then we have $d_p(L)=\sum_{i=1}^t c_i\frac{p^i-1}{p-1}$.

Lemma 2.9. *Let $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition, p a prime number and L a positive integer. Then for any $G \in R[x_1, \dots, x_n]$, we have $\left(\frac{\partial}{\partial f_i}\right)^L G \in p^{d_p(L)} R[x_1, \dots, x_n]$.*

Proof. By Lemma 2.7, letting $N = d_p(L)$, we have an expression

$$G \equiv \sum_{0 \le \alpha_1, \dots, \alpha_n < p^N} a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) f^\alpha \mod p^N.$$

By Leibniz rule, we have

$$\left(\frac{\partial}{\partial f_i}\right)^L G \equiv \sum_{0 \le \alpha_1, \dots, \alpha_n < p^N, s+t=L} \binom{L}{s} \left(\frac{\partial}{\partial f_i}\right)^s a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) \left(\frac{\partial}{\partial f_i}\right)^t f^\alpha \mod p^N.$$

We have $\frac{\partial}{\partial f_i} a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) \equiv 0 \mod p^N$ and hence $\left(\frac{\partial}{\partial f_i}\right)^s a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) \equiv 0 \mod p^N$ for $s > 0$. On the other hand, when $s = 0$, we have $\left(\frac{\partial}{\partial f_i}\right)^L f^\alpha = L!\binom{\alpha_i}{L} f^{\alpha - Le_i} \equiv 0 \mod p^{d_p(L)}$. Therefore we conclude that $\left(\frac{\partial}{\partial f_i}\right)^L G \in p^{d_p(L)} R[x_1, \dots, x_n]$. □

Proposition 2.10. *Suppose $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition. For $G \in R[x_1, \dots, x_n]$, we have $\left(\frac{\partial}{\partial f_i}\right)^L G \in L! R[x_1, \dots, x_n]$.*

Proof. By Lemma 2.9, for each prime $p \le L$, there exists a polynomial $\varphi_p \in R[x_1, \dots, x_n]$ such that $\left(\frac{\partial}{\partial f_i}\right)^L G = p^{d_p(L)} \varphi_p$. The GCD of the integers $\{L!/(p^{d_p(L)}) \mid p \le L\}$ is 1, hence we can find integers m_p so that $\sum m_p(L!/(p^{d_p(L)})) = 1$. Taking the polynomial $\varphi = \sum m_p \varphi_p$, we have

$$L!\varphi = L! \sum m_p \varphi_p = \sum m_p \frac{L!}{p^{d_p(L)}} p^{d_p(L)} \varphi_p = \left(\frac{\partial}{\partial f_i}\right)^L G.$$

We are done. □

Corollary 2.11. *If $L! \in R$ is a non-zero-divisor and $F_1, \dots, F_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition, then an R homomorphism $\frac{1}{L!}\left(\frac{\partial}{\partial F_i}\right)^L : R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ is canonically determined. If moreover there is a ring homomorphism $R \to S$ such that S has a characteristic p^e where $p > 0$ is a prime number, when we set f_i to be the image of F_i and $N := e + d_p(L)$, the induced homomorphism $S[x_1, \dots, x_n] \to S[x_1, \dots, x_n]$ sends $g = \sum_{0 \le \alpha_1, \dots, \alpha_n < p^N} a_\alpha \cdot (x_1^{p^N}, \dots, x_n^{p^N}) f^\alpha$ to $\sum_{0 \le \alpha_1, \dots, \alpha_n < p^N} a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) \binom{\alpha_i}{L} f^{\alpha - Le_i}$. In particular, the induced homomorphism is independent of the choice of R and F_i, if we start from S and f_i.*

PROOF. The well-definedness of $\frac{1}{L!}\left(\frac{\partial}{\partial F_i}\right)^L$ is obvious. Take any preimage $G \equiv \sum_{0 \le \alpha_1, \dots, \alpha_n < p^N} A_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) F^\alpha \mod p^N$ of g, we have

$$\frac{1}{L!}\left(\frac{\partial}{\partial F_i}\right)^L G \equiv \sum_{0 \le \alpha_1, \dots, \alpha_n < p^N} A_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) \binom{\alpha_i}{L} F^{\alpha - Le_i} \mod p^N. \qquad \square$$

DEFINITION 2.12. Let $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition. When R has a characteristic p^e with a prime number p, we define $\partial_{f_i}^{[L]} : R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ to be an R homomorphism sending $g = \sum_{0 \le \alpha_1, \dots, \alpha_n < p^N} a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) f^\alpha$ to $\sum_{0 \le \alpha_1, \dots, \alpha_n < p^N, \alpha_i \ge L} a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) \binom{\alpha_i}{L} \times f^{\alpha - Le_i}$, with $N = e + d_p(L)$. Also when $L!$ is a non-zero-divisor in R, we define $\partial_{f_i}^{[L]} : R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ to be the unique R homomorphism such that $L! \partial_{f_i}^{[L]} = \left(\frac{\partial}{\partial f_i}\right)^L$.

Definition 2.12 will be generalized to any ring R (see Definition 3.16 for the general R, and Definition 3.13 for the case R finitely generated over $\mathbf{Z}$), with properties as in Theorem 2.13 below. The proof of Theorem 2.13 will be postponed until the next section (see Remark 3.17).

THEOREM 2.13. *For each set of polynomials $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ which satisfies the Jacobian condition, there is an R endmorphism $\partial_{f_i}^{[L]} : R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ which satisfies the following properties;*

(1) *If R has characteristic p^e with a prime number p, $\partial_{f_i}^{[L]}$ coincides with the one defined in Definition 2.12;*

(2) *if $L!$ is non-zero-divisor in R, then $\partial_{f_i}^{[L]}$ coincides with the one defined in Definition 2.12;*

(3) *$\partial_{f_i}^{[L]}$ is functorial. Namely, when $\varphi : R \to S$ is a ring homomorphism, then for any $g \in R[x_1, \dots, x_n]$, we have $\varphi(\partial_{f_i}^{[L]} g) = \partial_{\varphi(f_i)}^{[L]} \varphi(g)$.*

Moreover, the system to associate R homomorphisms $\{\partial_{f_i}^{[L]}\} : R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ to the polynomials $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ with Jacobian condition is unique, if this system satisfies the properties (1) *and* (3) *above.*

LEMMA 2.14. *Let R be a ring of prime characteristic $p > 0$, and assume that $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition. Define X_i to be $X_i = x_i^{p^r} \in R[x_1, \dots, x_n]$. Then the polynomials $f_1^{p^r}, f_2^{p^r}, \dots, f_n^{p^r} \in R[X_1, \dots, X_n]$ satisfy the Jacobian condition.*

PROOF. By Proposition 2.4, each x_i can be written as $x_i = \sum a_\alpha(x_1^p, \dots, x_n^p) f^\alpha$. Take the p^r-th power. We see that $x_i^{p^r} \in S[x_1^{p^{r+1}}, \dots, x_n^{p^{r+1}}, f_1^{p^r}, \dots, f_n^{p^r}]$, therefore $R[X_1, \dots, X_n] = S[X_1^p, \dots, X_n^p, f_1^{p^r}, \dots, f_n^{p^r}]$. By

Proposition 2.4 again, we conclude that $f_1^{p^r}, \dots, f_n^{p^r}$ satisfy the Jacobian condition. $\square$

Proposition 2.15. *Suppose $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition. When the characteristic of R is a prime number $p > 0$, then for $g = \sum_{0 \le \alpha_1, \dots, \alpha_n < p^r} a_\alpha(x_1^{p^r}, \dots, x_n^{p^r}) f^\alpha$, we have*

$$\partial_{f_i}^{[p^r]} g = \sum_{0 \le \alpha_1, \dots, \alpha_n < p^r} \left(\frac{\partial}{\partial f_i^{p^r}} \right) a_\alpha(x_1^{p^r}, \dots, x_n^{p^r}) f^\alpha$$

where by Lemma 2.14, $f_1^{p^r}, \dots, f_n^{p^r} \in R[x_1^{p^r}, \dots, x_n^{p^r}]$ satisfy the Jacobian condition, and $\frac{\partial}{\partial f_i^{p^r}} : R[x_1^{p^r}, \dots, x_n^{p^r}] \to R[x_1^{p^r}, \dots, x_n^{p^r}]$ is the R homomorphism defined by Definition 2.3.

Proof. We may assume that $g = a(x_1^{p^N}, \dots, x_n^{p^N}) f^{p^r \beta + \alpha}$, where $N = 1 + d_p(p^r)$ and $0 \le \alpha_1, \dots, \alpha_n < p^r$. Applying $\partial_{f_i}^{[p^r]}$ to g, we obtain $a(x_1^{p^N}, \dots, x_n^{p^N}) \binom{p^r \beta_i + \alpha_i}{p^r} f^{p^r \beta - p^r e_i + \alpha}$, which equals to $a(x_1^{p^N}, \dots, x_n^{p^N}) \cdot \beta_i f^{p^r(\beta - e_i)} f^\alpha$, because $\binom{p^r \beta_i + \alpha_i}{p^r} \equiv \beta_i \bmod p$ if $0 \le \alpha_i < p^r$. $\square$

Corollary 2.16. *Suppose $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition. When the characteristic of R is a prime number $p > 0$, we have*

$$\bigcap_{L > 0,\, i > t} \operatorname{Ker} \partial_{f_i}^{[L]} = \bigcap_{r > 0} R[x_1^{p^r}, \dots, x_n^{p^r}, f_1, f_2, \dots, f_t].$$

Proof. If $g \in \bigcap_{r>0} R[x_1^{p^r}, \dots, x_n^{p^r}, f_1, f_2, \dots, f_t]$, then g can be written as a linear combination of $a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) f^\alpha$ with $\alpha_1 = \dots = \alpha_t = 0$ and N arbitrary large. Hence its image by $\partial_{f_i}^{[L]}$ with $i > t$ is zero for $d_p(L) < N$, therefore g is in the left hand side.

Conversely, assume that g is in the left hand side. It is easy to check that if $\partial_{f_i}^{[1]} g = 0$ for $i = t+1, t+2, \dots, n$, then $g \in R[x_1^p, \dots, x_n^p, f_1, \dots, f_t]$. Proceeding by induction on r, assume that $g \in R[x_1^{p^r}, \dots, x_n^{p^r}, f_1, f_2, \dots, f_t]$, namely we can write

$$g = \sum_{0 \le \alpha_{t+1}, \dots, \alpha_n < p^r} a_\alpha(x_1^{p^r}, \dots, x_n^{p^r}) f_1^{\alpha_1} \dots f_t^{\alpha_t}$$

for some $r > 0$, with $r = 1$ case already checked. We apply $\partial_{f_i}^{[p^r]}$ to g to obtain $\sum \left(\frac{\partial}{\partial f_i^{p^r}} \right) a_\alpha(x_1^{p^r}, \dots, x_n^{p^r}) f_1^{\alpha_1} \dots f_t^{\alpha_t} = 0$ by Proposition 2.15. By the uniqueness of such a representation (Proposition 2.4), we have $\partial_{f_i^{p^r}}^{[1]} a_\alpha(x_1^{p^r}, \dots, x_n^{p^r}) = 0$ for $i = t+1, t+2, \dots, n$, hence we have $a_\alpha(x_1^{p^r}, \dots, x_n^{p^r}) \in R[x_1^{p^{r+1}}, \dots, x_n^{p^{r+1}}, f_1^{p^r}, \dots, f_t^{p^r}]$, which shows that the $r+1$ case holds. We are done. $\square$

3. Higher derivations

In this section, we prove Theorem 2.13.

LEMMA 3.1. *Let R be a ring, and assume that $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition. Then a polynomial $g \in R[x_1^{p^{N-j}}, \dots, x_n^{p^{N-j}}]$ can be written as $g = \sum_{0 \le \alpha_1, \dots, \alpha_n < p^j} a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) f^{p^{N-j}\alpha} + ph(x_1, \dots, x_n)$.*

PROOF. By Lemma 2.14, $f_1^{p^{N-j}}, \dots, f_n^{p^{N-j}}$ satisfy the Jacobian condition in $(R/pR)[x_1^{p^{N-j}}, \dots, x_n^{p^{N-j}}]$, hence by Corollary 2.6, we have the desired expression. □

LEMMA 3.2. *Let $\psi_1, \dots, \psi_r \in R[x_1, \dots, x_n]$ be polynomials. Then any polynomial $\varphi \in R[\psi_1^{p^N}, \dots, \psi_r^{p^N}] \subset R[x_1, \dots, x_n]$ can be written as $\varphi = \sum_{i=0}^N p^i \varphi_i(x_1^{p^{N-i}}, \dots, x_n^{p^{N-i}})$.*

PROOF. By multinomial expansion formula, if $g = \sum_{j=1}^r a_{\alpha_j} x^{\alpha_j}$, we have

$$g^{p^N} = \sum_{d_1 + \cdots + c_r = p^N} \frac{p^N!}{d_1! d_2! \dots d_r!} \prod (c_{\alpha_j} x^{\alpha_j})^{d_j}$$

with p^i divides $\frac{p^N!}{d_1! d_2! \dots d_r!}$ if one of d_j's is not divisible by p^{N-i+1}, hence g^{p^N} is in $\sum_{i=0}^N p^i R[x_1^{p^{N-i}}, \dots, x_n^{p^{N-i}}]$. The polynomial φ is a linear combination of such polynomials, therefore it is also in $\sum_{i=0}^N p^i R[x_1^{p^{N-i}}, \dots, x_n^{p^{N-i}}]$. □

LEMMA 3.3. *If $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition, then for each multi-index α, we can write*

$$f^{p^N\alpha} = g_0(x_1^{p^N}, \dots, x_n^{p^N}) + \sum_{i=1}^N \left(\sum_{p^{N-i} \mid \beta,\, 0 \le \beta_1, \dots, \beta_n < p^N} p^i a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) f^\beta \right).$$

PROOF. As $f^{p^N\alpha} \bmod p$ is in $(R/pR)[x_1^{p^N}, \dots, x_n^{p^N}]$, we can find a polynomial $g_0(x_1^{p^N}, \dots, x_n^{p^N})$ such that $f^{p^N\alpha} - g_0 \in pR[x_1, \dots, x_n]$. By Lemma 3.2, we can write $f^{p^N\alpha} = g_0(x_1^{p^N}, \dots, x_n^{p^N}) + \sum_{i=1}^N p^i g_i(x_1^{p^{N-i}}, \dots, x_n^{p^{N-i}})$. We will show that $f^{p^N\alpha}$ can be written as

$$f^{p^N\alpha} = g_0(x_1^{p^N}, \dots, x_n^{p^N}) + \sum_{i=1}^{j-1} \left(\sum_{p^{N-j+1} \mid \beta,\, 0 \le \beta_1, \dots, \beta_n < p^N} p^{j-1} a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) f^\beta \right)$$
$$+ \sum_{i=j}^N p^i g_i(x_1^{p^{N-i}}, \dots, x_n^{p^{N-i}})$$

by induction on j. Assuming the j-th case, by Lemma 3.1, we can write

$$g_j(x_1^{p^{N-j}}, \dots, x_n^{p^{N-j}}) \equiv \sum_{0 \le \gamma < p^j} a_\gamma(x_1^{p^N}, \dots, x_n^{p^N}) f^{p^{N-j}\gamma} \quad \bmod p.$$

By Lemma 3.2, $g_j - \sum a_\gamma f^{p^{N-j}\gamma} \in R[x_1^{p^{N-j}}, \dots, x_n^{p^{N-j}}, f_1^{p^{N-j}}, \dots, f_n^{p^{N-j}}]$ is in

$$\sum_{i=j}^{N} p^{i-j} R[x_1^{p^{N-i}}, \dots, x_n^{p^{N-i}}] \cap pR[x_1, \dots, x_n] = \sum_{i=j+1}^{N} p^{i-j} R[x_1^{p^{N-i}}, \dots, x_n^{p^{N-i}}]$$

substituting which gives the $j+1$-st expression, and the induction (hence the proof) is complete. □

Lemma 3.4. *Let R be a ring with characteristic a prime power $p^e > 0$, and $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ polynomials with the Jacobian condition. Let us write f^α as $f^\alpha = \sum_{0 \le \beta < p^N} a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) f^\beta$. If p^{N-j+1} does not divide $\alpha_i - \beta_i$ for each i, then $a_\beta \in p^j R[x_1^{p^N}, \dots, x_n^{p^N}]$.*

Proof. We will show that f^α can be written as

$$f^\alpha = \sum_{i=0}^{j-1} \left(\sum_{p^{N-i} | (\alpha - \beta),\, 0 \le \beta_1, \dots, \beta_n < p^N} p^i a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) f^\beta \right)$$
$$+ \sum_{i=j}^{N} \left(\sum_{p^{N-i} | (\alpha - \beta)} p^i a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) f^\beta \right)$$

by induction on j. Take a multi-index α_0 with $\alpha_0 \equiv \alpha \bmod p^N$ and $0 \le \alpha_0 < p^N$. Then writing $\alpha = \alpha_0 + p^N \gamma$, we have $f^\alpha = f^{\alpha_0} f^{p^N \gamma}$, and substituting the expression of $f^{p^N \gamma}$ of Lemma 3.3, we prove the case for $j = 1$. Assuming the case for j, for each f^β with $p^{N-j} | \beta$ and $\beta \not< p^N$, we write $\beta = \beta_0 + p^N \delta$, $0 \le \beta_0 < p^N$, and substitute the expression of $f^{p^N \delta}$ of Lemma 3.3 to $f^\beta = f^{\beta_0} f^{p^N \delta}$. Then we obtain the expression for $j+1$, and the induction completes. □

Lemma 3.5. *Assume that R has a prime power charactersitic p^e, and $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition. Suppose that the multi-index α is such that $0 \le \alpha_1, \alpha_2, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_n < p^N$, $p^N \le \alpha_i < p^N + L$ with $L > 0$ an integer and $N = e + d_p(L)$. When we write $f^\alpha = \sum_{0 \le \beta_1, \dots, \beta_n < p^N} a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) f^\beta$, then we have*

$$\binom{\alpha_i}{L} f^{\alpha - Le_i} = 0 = \sum_{0 \le \beta_1, \dots, \beta_n < p^N} a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) \binom{\beta_i}{L} f^{\beta - Le_i}.$$

Proof. The assumption $p^N \le \alpha_i < p^N + L$ implies that $p^{N - d_p(L)} = p^e$ divides $\binom{\alpha_i}{L}$, hence the left hand side is 0. For the right hand side, for each

β, choose j so that $p^{N-j} \mid (\alpha-\beta)$ but $p^{N-j+1} \nmid (\alpha-\beta)$. If $N-j < d_p(L)$, then we have $j > e$, and by Lemma 3.4, we have $a_\beta = 0$. On the other hand, if $N-j \geq d_p(L)$, then $\binom{\beta_i}{L}$ is divisible by $p^{N-j-d_p(L)}$, and again by Lemma 3.4, $a_\beta(x_1^{p^N}, \dots, x_n^{p^N})$ is divisible by p^j, hence $\binom{\beta_i}{L} a_\beta$ is divisible by $p^{N-d_p(L)} = 0$, hence the right hand side is also 0. $\square$

PROPOSITION 3.6. *Assume that R has a prime power characteristic p^e. If $g = \sum_\alpha a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) f^\alpha \in R[x_1, \dots, x_n]$ with α not necessarily in the range of $0 \leq \alpha < p^N$, and $N = e + d_p(L)$, then we have*

$$\partial_{f_i}^{[L]} g = \sum a_\alpha(x_1^{p^N}, \dots, x_n^{p^N}) \binom{\alpha_i}{L} f^{\alpha - Le_i}$$

PROOF. By linearity, we may assume that $g = f^\alpha$. First, we treat the case where $\alpha_i \geq L$. When we write $f^{\alpha-Le_i} = \sum_{0 \leq \beta_1, \dots, \beta_n < p^N} a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) f^\beta$, then $\binom{\alpha_i}{L} f^{\alpha - Le_i} = \sum a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) \binom{\alpha_i}{L} f^\beta$. For each β, take j so that $\alpha - Le_i - \beta$ is divisible by p^{N-j}, but not by p^{N-j+1}. If $j \geq e$, then by Lemma 3.4, $a_\beta = 0$. On the other hand, if $j < e$, then $\binom{\beta_i + L}{L} \equiv \binom{\alpha_i}{L}$ mod $p^{N-j-d_p(L)}$ and $p^j | a_\beta$ by Lemma 3.4 again, which imply that $\binom{\alpha_i}{L} f^{\alpha-Le_i} = \sum a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) \binom{\beta_i+L}{L} f^\beta$. Because $f = \sum_{0 \leq \beta < p^N} a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) f^{\beta + Le_i}$, we may assume that $0 \leq \alpha_k < p^N$ for $k \neq i$ and $p^N \leq \alpha_i < p^N + L$ from the beginning. But this speicial case is already proved in Lemma 3.5.

We still need to prove Proposition for the case $\alpha_i < L$. In that case, when we write $f^\alpha = \sum_{0 \leq \beta_1, \dots, \beta_n < p^N} a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) f^\beta$, if p^{N-j+1} does not divide $\alpha - \beta$, then a_β is divisible by p^j by Lemma 3.4. Also if p^{N-j} divides $\alpha - \beta$, then $\binom{\beta_i}{L}$ is divisible by $p^{N-j-d_p(L)}$. Hence choosing j to be such that $\alpha - \beta$ is divisible by p^{N-j} but not by p^{N-j+1}, we conclude that each $a_\beta \binom{\beta_i}{L}$ is divisible by $p^{N-d_p(L)} = 0$. We have $\partial_{f_i}^{[L]} f^\alpha = 0 = \sum a_\beta(x_1^{p^N}, \dots, x_n^{p^N}) \binom{\beta_i}{L} f^{\beta^L e_i}$ in this case. $\square$

LEMMA 3.7. *Let $\varphi : R \to S$ be a ring homomorphism, and assume that R has a prime power characteristic p^e. Let $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian Condition, $g \in R[x_1, \dots, x_n]$ a polynomial, and by abuse of notation, we write $\varphi : R[x_1, \dots, x_n] \to S[x_1, \dots, x_n]$ for the induced homomorphism with $\varphi(x_i) = x_i$. Then S has a prime power characteristic, $\varphi(f_1), \dots, \varphi(f_n) \in S[x_1, \dots, x_n]$ satisfy the Jacobian Condition, and we have the compatibility formula $\varphi(\partial_{f_i}^{[L]} g) = \partial_{\varphi(f_i)}^{[L]} \varphi(g)$.*

PROOF. The compatibility formula follows from Proposition 3.6. The rest is easy. $\square$

Proposition 3.8. *Let R be a Noetherian ring, and assume that $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition. For a prime number p and each integer $e > 0$, define the canonical homomorphism $\varphi_{p^e} : R[x_1, \dots, x_n] \to R/(p^e R)[x_1, \dots, x_n]$. Then for a polynomial $g \in R[x_1, \dots, x_n]$, the system of polynomials $\{\partial^{[L]}_{\varphi_{p^e}(f_i)} \varphi_{p^e}(g)\}_{e=1,2,\dots}$ forms an inverse system, and determines an element*

$$\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g) \in \left(\varprojlim_{e} R/p^e R \right) [x_1, \dots, x_n].$$

Proof. By Lemma 3.7, the higher derivations are compatible with the ring homomorphisms, hence the system $\{\partial^{[L]}_{\varphi_{p^e}(f_i)} \varphi_{p^e}(g)\}_{e=1,2,\dots}$ forms an inverse system. We need to show that the degrees are bounded, which implies that the inverse limit lies in the polynomial ring, in the ring of the power series.

Define an ideal $I \subset R$ by $I := \{r \in R \mid p^s r = 0 \text{ for some } s > 0\}$. As R is Noetherian, $p^e I = 0$ for some $e > 0$. Let $e' > e$, and take $c \in R/(p^{e'} R)$ to be the coefficient of x^α in $\partial^{[L]}_{\varphi_{p^{e'}}(f_i)} \varphi_{p^{e'}}(g)$, where the coefficients of x^α in both $\partial^{[L]}_{\varphi_{p^e}(f_i)} \varphi_{p^e}(g)$ and $\left(\frac{\partial}{\partial f_i}\right)^L g$ are zero. We will show that $c = 0$, which implies the boundedness of the degree.

Let $e'' = e' + d_p(L)$, then by Lemma 3.7, c is the image of the coefficient $c_1 \in R/(p^{e''} R)$ of x^α in $\partial^{[L]}_{\varphi_{p^{e''}}(f_i)} \varphi_{p^{e''}}(g)$. Then $L! c_1$ is the coefficient of x^α in $\left(\frac{\partial}{\partial \varphi_{p^{e''}}(f_i)}\right)^L \varphi_{p^{e''}}(g)$, which is zero by the assumption of c. As $\frac{L!}{p^{d_p(L)}}$ is invertible in $R/(p^{e''} R)$, we have $p^{d_p(L)} c_1 = 0$. Let $\tilde{c}_1 \in R$ be a preimage of c_1, then we have $p^{d_p(L)} \widetilde{c_1} = p^{e''} \widetilde{c'}$ for some $\widetilde{c'} \in R$. Also the image of c_1 in $R/(p^e R)$ is zero by the assumption of c, hence we have $\widetilde{c_1} = p^e \tilde{c}$ for some $c \in R$. Hence we have $p^{e''} \widetilde{c'} = p^{d_p(L)} \widetilde{c_1} = p^{d_p(L)} p^e \tilde{c}$, therefore $p^{e + d_p(L)} (\tilde{c} - p^{e' - e} \widetilde{c'}) = 0$, which means $\tilde{c} - p^{e'-e} \widetilde{c'} \in I$, hence $p^e (\tilde{c} - p^{e'-e} \widetilde{c'}) = 0$, and we obtain $\widetilde{c_1} = p^e \tilde{c} = p^{e'} \widetilde{c'}$. We conclude $c = \widetilde{c_1} \bmod p^{e'} R = 0$ as desired. □

The following result is well known.

Lemma 3.9. *Let R be a ring finitely generated over $\mathbf{Z}$. If $m \subset R$ is a maximal ideal, then the characteristic of R/m is positive.* □

Lemma 3.10. *Let R be a finitely generated ring over $\mathbf{Z}$, then the canonical homomorphism*

$$\varphi : R[x_1, \dots, x_n] \to \prod_{p} \varprojlim_{e} R/(p^e R)[x_1, \dots, x_n]$$

where p runs over all prime numbers, is injective.

Proof. It is enough to show that $R \to \prod_p \varprojlim_e R/(p^e R)$ is injective. Let $r \in R$ be a non-zero element, $I = \mathrm{ann}(r) \subset R$ be the annihilator ideal, and $m \supset I$ be any maximal ideal. By Lemma 3.9, the characteristic of R/m is positive, say p. We will show that the image of r in $\varprojlim_e R/(p^e R)$ is non-zero. Assuming to the contrary, taking the ideal $J = \bigcap p^e R$, we suppose that $r \in J$. Let $s_1, \dots, s_t$ be a set of generators of the ideal J, then because $J = pJ = (ps_1, \dots, ps_t)$, there is a matrix $A \in M_t(R)$ such that $pA\begin{pmatrix} s_1 \\ \vdots \\ s_t \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_t \end{pmatrix}$. Multiplying the adjoint matrix of $I - pA$ from the left side, we conclude that $\det(I - pA)J = 0$, hence $\det(I - pA)r = 0$, so we have $\det(I - pA) \in I$. On the other hand, we have $\det(I - pA) \equiv 1 \bmod p$, hence one can find an element $u \in R$ so that $1 - pu = \det(I - pA) \in I \subset m \ni p$, a contradiction. □

Lemma 3.11. *Let R be a finitely generated ring over $\mathbf{Z}$, $N \in \mathbf{Z}$ a positive integer, and consider the homomorphism $\varphi : R \to \prod_p \varprojlim_e R/(p^e R)$, then φ induces an isomorphism from* $\mathrm{ann}(N) \subset R$ *to* $\mathrm{ann}(N) \subset \prod_p \varprojlim_e R/(p^e R)$.

Proof. By Lemma 3.10, φ is injective, so we need only to show the surjectivity of $\varphi_{|\mathrm{ann}(N)}$. Each $\varprojlim_e R/(1p^e R)$ has only torsion of the order some power of p, so we may assume that $N = p^d$, and consider the homomorphism $\varphi_p : R \to \varprojlim_e R/(p^e R)$. Let $\{r_1, r_2, \dots\} \in \mathrm{ann}(p^d) \subset \varprojlim_e R/(p^e R)$, with $r_i \in R/(p^i R)$. First, we claim that one can find a preimage $\tilde{r}_i \in R$ of r_i so that $p^d \tilde{r}_i = 0$. Let $\tilde{r}'_i \in R$ be any preimage for each r_i. Because $\{r_1, r_2, \dots\}$ is an inverse system, if $i > j$, we have $\tilde{r}'_i \equiv \tilde{r}'_j \bmod p^j R$. Also, because $p^d r_i = 0$, one can find $s_i \in R$ so that $p^d \tilde{r}'_i = p^i s_i$ for each i. Let us take $\tilde{r}_i := \tilde{r}'_{i+d} - p^i s_{i+d}$, then $\tilde{r}_i$ is a preimage of r_i, and $p^d \tilde{r}_i = p^d \tilde{r}'_{i+d} - p^{i+d} s_{i+d} = 0$.

Similarly to the proof of Proposition 3.8, let us take the ideal $I := \{r \in R \mid p^s r = 0 \text{ for some } s > 0\}$, then for some $e > 0$, we have $p^e I = 0$. We claim that if $i \geq j \geq e$, then $\tilde{r}_i = \tilde{r}_j$. Since $\{r_1, r_2, \dots\}$ forms an inverse system, we have $\tilde{r}_j \equiv \tilde{r}_i \bmod p^j R$, hence there is some $t \in R$ such that $\tilde{r}_i - \tilde{r}_j = p^j t$. As $p^d \tilde{r}_i = p^d \tilde{r}_j = 0$, we have $p^d(\tilde{r}_i - \tilde{r}_j) = p^{d+jt=0}$, so t is in the ideal I. Therefore, we have $\tilde{r}_i - \tilde{r}_j = p^j t = p^{j-e} p^e t = 0$, because $p^e I = 0$.

By replacing $\tilde{r}_i$ with $i < e$ by $\tilde{r}_e$, we conclude that our torsion element $\{r_1, r_2, \dots\}$ is the image of $\tilde{r}_e$, a torsion element in R. We are done. □

Proposition 3.12. *Let R be a finitely generated ring over $\mathbf{Z}$, $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition, and $g \in R[x_1, \dots x_n]$ a polynomial,* *then* $\prod_p (\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g))$ *is in* $\prod_p \varprojlim_e R/(p^e R)[x_1, \dots, x_n]$, *and it lies in the image of the canonical ring homomorphism* $\varphi : R[x_1, \dots, x_n] \to \prod_p \varprojlim_e R/(p^e R)[x_1, \dots, x_n]$. *Morever, if* $L!$ *is invertible in* R, *then we have* $\varphi(\partial^{[L]}_{f_i} g) = \prod_p (\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g))$ *defined in Definition* 2.12.

Proof. Each $(\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g))$ is a polynomial by Proposition 3.8. Also for $p > L$, $L!$ is invertible in each $R/(p^e R)$, hence $(\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g))$ is the inverse limit of $\frac{1}{L!} \varphi_{p^e}\left(\left(\frac{\partial}{\partial f_i}\right)^L g\right)$, hence the degree of $\prod_p (\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g))$ is bounded, and is a polynomial.

By Proposition 2.10, we can write $\left(\frac{\partial}{\partial f_i}\right)^L g = L!h$ for some $h \in R[x_1, \dots, x_n]$, and then we have $L!\left(\varphi(h) - \prod_p (\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g))\right) = 0$. By Lemma 3.11, there is $h_1 \in R[x_1, \dots, x_n]$ such that $\varphi(h_1) = \varphi(h) - \prod_p (\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g))$, hence $\prod_p (\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g))$ equals $\varphi(h - h_1)$, in the image of φ. If $L!$ is invertible in R, then $h = \partial^{[L]}_{f_i} g$, and $h_1 = 0$. □

Definition 3.13. When R is finitely generated ring over $\mathbf{Z}$ and $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian condition, then for $g \in R[x_1, \dots, x_n]$, we define the higher derivation $\partial^{[L]}_{f_i} g$ to be the preimage of $\prod_p (\partial^{[L]}_{\varphi_{p^\infty}(f_i)} \varphi_{p^\infty}(g))$.

Remark 3.14. By Proposition 3.12, the preimage exists, and by Lemma 3.10, it is unique. If $L!$ is invertible in R, then this definition coincides with Definition 2.12 by Proposition 3.12. Also if R has a prime power characteristic p^e, then $\prod_p \left(\varprojlim_e R/(p^e R)[x_1, \dots, x_n]\right) \simeq \varprojlim_e R/(p^e R)[x_1, \dots, x_n] \simeq R[x_1, \dots, x_n]$, and by the construction, Definition 3.13 and Definition 2.12 agree.

Lemma 3.15. *Let* $\psi : R \to S$ *be a homomorphism between rings finitely generated over* $\mathbf{Z}$, $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ *satisfy the Jacobian Condition, and* $g \in R[x_1, \dots, x_n]$ *a polynomial. By abuse of notation, let* $\psi : R[x_1, \dots, x_n] \to S[x_1, \dots, x_n]$ *be the extension of* ψ, *defined by* $\psi(x_i) = x_i$. *Then* $\psi(\partial^{[L]}_{f_i} g) = \partial^{[L]}_{\psi(f_i)} \psi(g)$ *holds.*

Proof. By the definition of the higher derivation, we may assume that R has a prime power characteristic, which case is already proved in Lemma 3.7. □

Definition 3.16. Let R be any ring, $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ satisfy the Jacobian Condition, and $g \in R[x_1, \dots, x_n]$ a polynomial. Take a ring injection $\psi : S \to R$ so that $\psi(S)[x_1, \dots, x_n]$ contains $f_1, \dots, f_n$, g and $\det\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j}^{-1}$. Let $\tilde{f_i}$ and $\tilde{g}$ be the preimages of f_i and g respectively, and define $\partial_{f_i}^{[L]}(g)$ to be the image of $\partial_{\tilde{f_i}}^{[L]}(\tilde{g})$.

Remark 3.17. By Lemma 3.15, this definition is well defined, independent of the choice of the injection ψ. By this definition, Theorem 2.13 obviously holds.

4. SAGBI basis

Definition 4.1. Let k be a field. Throughout this section, fix a monomial order for the monomials in $k[x_1, \dots, x_n]$ (see [3]). For a k subalgebra $R \subset k[x_1, \dots, x_n]$, define $LM(R)$ to be $\{LM(f) \mid f \in R\}$, where $LM(f)$ is the leading monomial of f.

Lemma 4.2. *Let $S \subset R$ be k subalgebras of $k[x_1, \dots, x_n]$. If $LM(S) = LM(R)$, then $S = R$.*

Proof. Assume that S is a proper subalgebra of R. Take a polynomial $f \in R - S$ with $LM(f)$ minimal, which is possible because monomial order is a well ordering. As $LM(S) = LM(R)$, for some $g \in S$, we have $LM(g) = LM(f)$. Then for a suitable constant $c \in k^*$, $LM(f - cg) < LM(f)$, and $f - cg \in R - S$, a contradiction. □

Definition 4.3. Consider $LM(R)$ as a monoid under multiplication. When $\{LM(f_\lambda)\}_{\lambda \in \Lambda}$ generates $LM(R)$, the set $\{f_\lambda \mid \lambda \in \Lambda\}$ is called a SAGBI basis of R.

Remark 4.4. Even when R is a finitely generated k subalgebra of $k[x_1, \dots, x_n]$, it is possible that there is no finite SAGBI basis for R (see [8]).

Definition 4.5. Let p be a prime. For each $f \in k[x_1, \dots, x_n]$, consider $LM(f) = x^\alpha$ as a vector $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbf{Z}^n$. Polynomials $f_1, \dots, f_t \in k[x_1, \dots, x_n]$ are said to *have linearly independent degree modulo p*, if $\overline{LM(f_1)}, \dots, \overline{LM(f_t)} \in \mathbf{F}_p^n$ are linearly independent in the vector space over $\mathbf{F}_p$, where $\overline{LM(f_i)}$ is the image of $LM(f_i)$ by the natural map $\mathbf{Z}^n \to \mathbf{F}_p^n$.

Proposition 4.6. *Let k be a field with characteristic $p > 0$, and $r > 0$ an integer. If $f_1, \dots, f_n \in k[x_1, \dots, x_n]$ have linearly independent degree modulo p, then $\{x_1^{p^r}, \dots, x_n^{p^r}, f_1, \dots, f_n\}$ is a SAGBI basis of the k subalgebra $k[x_1^{p^r}, \dots, x_n^{p^r}, f_1, \dots, f_n] \subset k[x_1, \dots, x_n]$.*

PROOF. If $g \in k[x_1^{p^r}, \ldots, x_n^{p^r}, f_1, \ldots, f_n]$, we can write $g = \sum_{0 \le \beta_1, \ldots, \beta_n < p^r} a_\beta(x_1^{p^r}, \ldots, x_n^{p^r}) f^\beta$, because $f^{p^r\beta} \in k[x_1^{p^r}, \ldots, x_n^{p^r}]$ by the Frobenius map. We claim that the elements $LM(a_\beta(x_1^{p^r}, \ldots, x_n^{p^r}) f^\beta)$, $(0 \le \beta_1, \ldots, \beta_n < p^r)$, are all distinct, which implies that $LM(g) = \max LM(a_\beta(x_1^{p^r}, \ldots, x_n^{p^r}) f^\beta) \in \langle LM(x_1^{p^r}), \ldots, LM(x_n^{p^r}), LM(f_1), \ldots, LM(f_n) \rangle$.

Let $v_i = LM(f_i) \in \mathbf{Z}^n$, considered as a vector as in Definition 4.5. Assuming that $LM(a_\beta(x_1^{p^r}, \ldots, x_n^{p^r}) f^\beta) = LM(a_\gamma(x_1^{p^r}, \ldots, x_n^{p^r}) f^\gamma)$, we will show that $\beta = \gamma$. We have $\sum(\beta_i - \gamma_i)v_i \equiv 0 \mod p^r$. Let $\delta_i := \beta_i - \gamma_i$, then $\sum \delta_i v_i \equiv 0 \mod p^r$. We prove that each δ_i can be written as $\delta_i = p^j \delta_{i,j}$ with $\delta_{i,j} \in \mathbf{Z}$, $j = 0, 1, \ldots, r$ by induction on j. When $j = 0$, nothing is to be proved. Assume that $\delta_i = p^j \delta_{i,j}$ with $j < r$. Then since $\sum \delta_i v_i \equiv 0 \mod p^r$, we have $\sum \delta_{i,j} v_i \equiv 0 \mod p^{r^j}$. The vectors $\overline{v_i} := v_i \mod p$ are linearly independent over $\mathbf{F}_p$ by assumption, we have $\delta_{1,j} \equiv \delta_{2,j} \equiv \cdots \equiv \delta_{r,j} \equiv 0 \mod p$, the induction completes. Hence $\delta_i = \beta_i - \gamma_i$ is divisible by p^r, and because $0 \le \beta_i, \gamma_i < p^r$, we conclude that $\beta = \gamma$. $\square$

COROLLARY 4.7. *If $f_1, \ldots, f_t$ have linearly independent degree modulo $p > 0$, with p the charactersitic of k, then $\bigcap_{r>0} k[x_1^{p^r}, \ldots, x_n^{p^r}, f_1, \ldots, f_t] = k[f_1, \ldots, f_t]$.*

PROOF. Let $S = k[f_1, \ldots, f_t]$, and $R = \bigcap_{r>0} k[x_1^{p^r}, \ldots, x_n^{p^r}, f_1, \ldots, f_t]$, then obviously $S \subset R$. By Lemma 4.2, it is enougth to show that $LM(S) \supset LM(R)$. Let $g \in R$ be a non-zero polynomial, then for any $r > 0$, we have $g \in k[x_1^{p^r}, \ldots, x_n^{p^r}, f_1, \ldots, f_t]$. Pick r large enough so that the degree of g in x_i is less than p^r for all i. By Proposition 4.6, we have $LM(g) \in \langle LM(x_1^{p^r}), \ldots, LM(x_n^{p^r}), LM(f_1), \ldots, LM(f_t) \rangle$. But because $LM(g)$ is not divisible by $x_i^{p^r}$, actually $LM(g) \in \langle LM(f_1), \ldots, LM(f_t) \rangle \subset LM(S)$. We are done. $\square$

REMARK 4.8. If $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ satisfy the Jacobian condition and $f_1, \ldots, f_n$ have linearly independent degree modulo $p > 0$, the characteristic of k, then combining Corollary 4.7 with Corollary 2.6, one immediately proves the Jacobian conjecture in characteristic p in this special case. Unfortunately, from the proof of Corollary 4.7, it follows that $LM(S) = \langle LM(f_1), \ldots, LM(f_n) \rangle$, which means that our assumption holds only when $LM(f_1), \ldots, LM(f_n)$ are distinct degree 1 monomials, too trivial case to be mentioned.

REMARK 4.9. This section is the only "missing link" in the proof of Jacobian conjecture in general. All we have to solve is the following problem: Find a "good" condition for $f_1, \ldots, f_t$ so that $\bigcap_{r>0} k[x_1^{p^r}, \ldots, x_n^{p^r}, f_1, \ldots, f_t] = k[f_1, \ldots, f_t]$ holds.

5. Reduction to positive characteristic

CONJECTURE 5.1. *Weak Kernel Conjecture* WKC(n,t)*: Let k be a field of charecteristic* 0*, and $f_1,\dots,f_n \in k[x_1,\dots,x_n]$ satisfy the Jacobian Condition. Then we have*

$$\bigcap_{i>t} \operatorname{Ker} \frac{\partial}{\partial f_i} = k[f_1,\dots,f_t]$$

REMARK 5.2. When $t = n-1$, the Weak Kernel Conjecture WKC$(n,n-1)$ is the standard Kernel Conjecture for n variables, which implies the Jacobian Conjecture for $n-1$ variables. Conversely, the Jacobian Conjecture for n variables implies the standard Kernel Conjecture for n variables ([5]). If $t \ge s$, WKC(n,t) implies WKC(n,s).

The goal of this section (and this paper) is the following theorem.

THEOREM 5.3. *Let k be a field of characteristic* 0*, and $f_1,\dots,f_n \in k[x_1,\dots,x_n]$ satisfy the Jacobian Condition. Fix a monomial order for the monomials in $k[x_1,\dots,x_n]$. Consider $LM(f_1),\dots,LM(f_n)$ in $\mathbf{Z}^n$, as vectors in $\mathbf{Q}^n$. If $LM(f_1),\dots,LM(f_t)$ are linearly independent, then $\bigcap_{i>t} \operatorname{Ker} \frac{\partial}{\partial f_i} = k[f_1,\dots,f_t]$.*

COROLLARY 5.4. WKC$(n,1)$ *holds. In particular, it gives a new proof for the Kernel Conjecture for* 2 *variables.*

The key tool to reduce the WKC to positive characterisitc is the following lemma.

LEMMA 5.5. *Let k be a field of characteristic* 0*, $f_1,\dots,f_t,g \in k[x_1,\dots,x_n]$ polynomials, $a_1,\dots,a_s \in k^*$ finitely many non-zero elements in k, and N an positive integer. If $g \notin k[f_1,\dots,f_t]$, then there exists a subring $R \subset k$ which satisfies the following conditions.*

(1) *The ring R is finitely generated over $\mathbf{Z}$.*
(2) $f_1,\dots,f_t,g \in R[x_1,\dots,x_n]$.
(3) *The elements $a_1,\dots,a_s$ are invertible in R.*
(4) *For any maximal ideal $m \subset R$, let $\bar{f_1},\dots,\bar{f_t},\bar{g} \in R/m[x_1,\dots,x_n]$ be the canonical images of $f_1,\dots,f_t,g \in R[x_1,\dots,x_n]$, then $\bar{g} \notin R/m[\bar{f_1},\dots,\bar{f_t}]$.*
(5) *For any maximal ideal $m \subset R$, the characteristic of R/m is larger than N.*

PROOF. First, in order that $f_1,\dots,f_t,g \in R[x_1,\dots,x_n]$, the ring R must contain all the coefficients of f_i's and g's. Also to make sure that $a_1,\dots,a_s$ are invertible in R, R must contain $\frac{1}{a_1},\dots,\frac{1}{a_s}$.

Next, the assumption that $g \notin k[f_1,\dots,f_t]$ can be verified by the following calculation: Let $I \subset k[x_1,\dots,x_n,y_1,\dots,y_t]$ be the ideal generated by

$y_1 - f_1, \dots, y_t - f_t$. Take an elimination monomial order in $k[x_1, \dots, x_n, y_1, \dots, y_t]$, namely an order such that any monomial $y_1^{\alpha_1} \dots y_t^{\alpha_t}$ is smaller than each of $x_1, \dots, x_n$. Calculate the Groebner basis of the ideal I under this monomial order by Buchberger algorithm to obtain $\{h_1, \dots, h_s\}$, and apply the division algorithm to divide g by $\{h_1, \dots, h_s\}$. When r is the remainder, g is not in $k[f_1, \dots, f_t]$ if and only if r contains a term involving x, namely, $r \notin k[y_1, \dots, y_t]$.

In the calculation above, notice that we use the divisions by elements of k only finitely many times. We would like R to contain $\frac{1}{a}$ whenever we use the division by $a \in k$ in the calculation. Also in the final step of the verification of $g \notin k[f_1, \dots, f_t]$, we look up a term in the remainder r, which involves x, and see that its coefficient is non-zero. We would like R also to contain the multiplicative inverse of the coefficients.

Finally, to make sure that the characteristic of R/m is larger than N, it is enough that R contains $\frac{1}{N!}$, because the characteristic of R/m is positive by Lemma 3.9.

Once we generate the ring R by all these finitely many elements over $\mathbf{Z}$, the calculation to verify that $\bar{g} \notin R/m[\bar{f_1}, \dots, \bar{f_t}]$ proceeds exactly parallel to the verification of $g \notin k[f_1, \dots, f_t]$. $\square$

Lemma 5.6. *Let $f_1, \dots, f_t \in k[x_1, \dots, x_n]$ be polynomials, where the polynomial ring has some fixed monomial order. If the vectors $LM(f_1), \dots, LM(f_t) \in \mathbf{Z}^n \subset \mathbf{Q}^n$ are linearly independent, then there exists some integer N so that for any prime $p > N$, $f_1, \dots, f_t$ have linearly independent degree modulo p.*

Proof. Let $v_i = LM(f_i) \in \mathbf{Z}^n$ be the leading monomial of f_i considered as a vector. Because $v_1, \dots, v_t$ are linearly independent, there exists a non-zero $t \times t$ minor in the canonical matrix representation of $(v_1, \dots, v_t)$. One can choose N to be the absolute value of the determinant of the minor. $\square$

Now we are ready to prove our main theorem.

Proof (of Theorem 5.3). The inclusion $\bigcap_{i>t} \operatorname{Ker} \frac{\partial}{\partial f_i} \supset k[f_1, \dots, f_t]$ is obvious. Pick a polynomial $g \notin k[f_1, \dots, f_t]$. Assume that $\frac{\partial g}{\partial f_{t+1}} = \cdots = \frac{\partial g}{\partial f_n} = 0$, and we need to get some contradiction. Because $LM(f_1), \dots, LM(f_t)$ are linearly independent, by Lemma 5.6, there is some N such that for any prime $p > N$, the polynomials $f_1, \dots, f_t$ have linearly independent degree modulo p. Let a_i be the leading coefficient of f_i for $i = 1, 2, \dots, t$, and $a_{t+1} = \det\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j=1,\dots,n}$, and take the subring $R \subset k$ with $s = t+1$ as in Lemma 5.5. Let $m \subset R$ be any maximal ideal, $p > N$ the characteristic of R/m, and let $\bar{g}, \bar{f_1}, \dots, \bar{f_t}$ as in Lemma 5.5.

As $\det\left(\frac{\partial f_i}{\partial x_j}\right)$ is invertible in R, we can define the higher derivations $\partial_{f_i}^{[L]} g$,

$i = t+1, t+2, \dots, n$, $L > 0$, with R coefficients, and they are zero by the compatibility for $R \subset k$. Again by compatibility for $R \to R/m$, we have $\partial_{\bar{f}_i}^{[L]} \bar{g} = 0$ for $L > 0$, $i = t+1, \dots, n$, hence by Corollary 2.16, we have $\bar{g} \in \bigcap_{r>0} R/m[x_1^{p^r}, \dots, x_n^{p^r}, f_1, \dots, f_t]$. By Corollary 4.7, we have $\bigcap_{r>0} R/m[x_1^{p^r}, \dots, x_n^{p^r}, \bar{f}_1, \dots, \bar{f}_t] = R/m[\bar{f}_1, \dots, \bar{f}_t]$, contradicting the choice of R so that $\bar{g} \notin R/m[\bar{f}_1, \dots, \bar{f}_t]$. $\square$

References

[1] K. Adjamagbo, On separable algebras over a U.F.D. and the Jacobian conjecture in any characteristic, Automorphisms of Affine Spaces (Curacçao, 1994), Kluwer Acad. Publ., 1995, pp. 89–103.

[2] H. Bass, E. Connell and D. Wright, The Jacobian conjecture: Reduction of Degree and Formal Expansion of the Inverse, Bulletin of American Mathematical Society **7** (1982), 287–330.

[3] D. Cox, J. Little and D. O'Shea, Ideals, varieties, and algorithms, 2nd ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1997.

[4] D. Daigle and G. Freudenburg, A counterexample to Hilbert's fourteenth problem in dimension 5, J. Algebra **221** (1999), 528–535.

[5] A. van den Essen, Polynomial automorphisms and the Jacobian conjecture, Progress in Mathematics, vol. 190, Birkhäuser Verlag, Basel, 2000.

[6] A. Nowicki and M. Nagata, Rings of constants for k-derivations in $k[x_1, \dots, x_n]$, J. Math. Kyoto Univ. **28** (1988), 111–118.

[7] S. Okuda, Kernels of derivations in positive characteristic, Hiroshima Math. J. **34** (2004) (to appear).

[8] L. Robbiano and M. Sweedler, Subalgebra bases, Commutative algebra (Salvador, 1988), Lecture Notes in Math., vol. 1430, Springer, Berlin, 1990, pp. 61–87.

Shun-ichi Kimura
Department of Mathematics
Graduate School of Science
Hiroshima University
Higashihiroshima 739-8526, *Japan*
E-mail: kimura@math.sci.hiroshima-u.ac.jp

Shun-ichiro Okuda
Department of Mathematics
Graduate School of Science
Hiroshima University
Higashihiroshima 739-8526, *Japan*
Current Address: Tottori-NIshi Highschool
Tottori City Higashi-machi 2-112
680-0011 *Tottori Japan*
E-mail: okushn@ma4.seikyou.ne.jp