Publ. RIMS, Kyoto Univ.
23 (1987), 965-973

On a Stability Theorem for Local Uniformization in Characteristic p*

By

T. T. MOH**

Abstract

A 2nd numerical d is bounded under blow-ups.

Introduction

In [H, p. 123] Prof. H. Hironaka pointed out: "The point is that the associated Tschirnhausen polynomial undergoes the same law of transformation as the original polynomial under permissible blow-ups". For the notion of Tschirnhausen polynomials, or equivalently the approximate roots, the reader is referred to [A-M 1 & 2], [M] or [H]. As established by Prof. H. Hironaka the local uniformization problem in characteristic $p>0$ is to use monoidal transformations to resolve the singularity of an algebroid equation of the following form over $k[[x_1, \ldots, x_n]]$

$$z^{p^e}+\sum_{i=1}^{p^e} f_i(x_1, \ldots, x_n) z^{p^e-i}=0 \text{ with ord } (f_i) \geq i.$$

A specially important case is the following purely inseparable equation which is the topic of this article,

$$z^{p^e}+f_{p^e}(x_1, \ldots, x_n)=0$$

where $f_{p^e}(x_1, \ldots, x_n) \in k[[x_1, \ldots, x_n]]$ and $f_{p^e}(0, \ldots, 0)=0$. After some monoidal transformation the above equation will be transformed to

$$z^{p^e}+(\prod_{i=1}^{n} x_i^{m_i}) F(x_1, \ldots, x_n)=0$$

Communicated by H. Hironaka, October 14, 1986. Revised March 31, 1987.
* The research of this work was done with support of N. S. F.
** Mathematics Department, Purdue University, W. Lafayette, IN. 47907, U. S. A.

satisfying the characteristic p condition that the leading form of $(\prod_{i=1}^{n} x_i^{m_i})\ F(x_1, \dots, x_n)$ is not contained in $k[[x_1^{p^e}, \dots, x_n^{p^e}]]$. The following proposition has been established by us and will be published elsewhere.

Proposition A. *If* ord $F(x_1, \dots, x_n) = 0$ *then after finitely many blow-ups, the above singularity at the origin will have a smaller multiplicity.*

However, it can be shown that ord $F(x_1, \dots, x_n)$ *may increase in general. This is a serious blow to the hope that* ord $F(x_1, \dots, x_n)$ *will eventually drop to zero after monoidal transformations, and even open up the possibility that* ord $F(x_1, \dots, x_n)$ *may increase indefinitely and thus a counter example to resolution may be constructed! It is the purpose of this article to establish the following theorem:*

The Stability Theorem. *Let* $d=$ord $F(x_1, \dots, x_n)$. *After a permissible blowup, along a residually rational valuation* v *of the function field, say factor out* x_1, *and let* $\tilde{F}=x_1^{-d}F$. *Then* ord $\tilde{F} \leq d+p^{e-1}$ *and successive permissible blow-ups will not increase ord* $\tilde{F}$ *beyond the bound* $d+p^{e-1}$ *(in fact,* $d+p^r$, *see below) until it drops to* d *or less.*

We wish to express our deep thanks to Prof H. Hironaka for his kindness and enlightening guidances on this important problem of mathematics.

§ 1. A Proof of the Stability Theorem

Let k be an algebraically closed field of characteristic p and $R= k[[x_1, \dots, x_n]]$, the power series ring of n variables over k. Let

$$z^{p^e} + (\prod x_i^{m_i})\, F(x_1, \dots, x_n) = 0$$

be a purely inseparable equation to be resolved with $F(x_1, \dots, x_n) \in R$, Let $d=$ord $F(x_1, \dots, x_n)$ and

$$F(x_1, \dots, x_n) = F_d(x_1, \dots, x_n) + \text{higher terms}.$$

If $m_i \geq p^e$ then we may replace z by z/x_i and cut down m_i by p^e. Moreover, a translation of the form $z \to z+g$ will remove or change the p^e-th power part of $(\Pi x_i^{m_i})F_d(x_1, \dots, x_n)$. We shall keep these two operations in mind.

Our basic assumption is $(\Pi x_i^{m_i})F_d \notin R^{p^e}$ and $0 \leq m_i < p^e$. Let v be any residually rational valuation given. We shall make the following definition and convention.

Definition. *An ideal P is said to be a permissible center if there is a system of parameters $\{y_1, \dots, y_n\}$ such that* (1) *all x_i's with $m_i \neq 0$ are among them,* (2) *a part of them generate P,* (3) *$f \in P^d$ where $d = \mathrm{ord}\ F$. Note that if $P = (y_1, \dots, y_s)$ then the leading form F_d of F is a homogeneous polynomial of degree d in the leading form of $\{y_1, \dots, y_s\}$. We assume that $\{y_1, \dots, y_n\}$ is $\{x_1, \dots, x_n\}$.*

Convention. After making a choice of the order of n variables as $x_1, \dots, x_n$, then in the monoidal transformation we always factor out the x_i satisfying the following conditions: (1) x_i is in the center P of the permissible monoidal transformation; (2) $v(x_i) = \min\{v(\alpha) : \alpha \in P\}$; (3) the integer i is the minimal integer satisfying condition (2). With such an x_i, the monoidal transformation will be of the following form:

$$\begin{aligned} x_i &= \bar{x}_i \\ x_j &= \bar{x}_i \bar{x}_j & \forall j < i,\ x_j \in P \\ x_k &= \bar{x}_i(\bar{x}_k + \alpha_k) & \forall k > i,\ x_k \in P \\ x_l &= \bar{x}_l & \forall x_l \notin P \end{aligned}$$

where $\alpha_k \in k$.

To simplify our notation we may assume that $i = 1$, namely, $x_1 \in P$ and

$$v(x_1) \leq v(x_j) \qquad \forall x_j \in P.$$

Moreover we shall use the subdivision of the set of variables $\{x_1, \dots, x_n\} = \{x_1\} \cup X \cup Y \cup Z$ where

$$\begin{aligned} X &= \{x_i : x_i \in P,\ {}_i \neq 1,\ m_i = 0 \text{ or } v(x_i) > v(x_1)\} \\ Y &= \{x_j : x_j \in P,\ {}_j \neq 1,\ m_j \neq 0 \text{ and } v(x_j) = v(x_1)\} \\ Z &= \{x_l : x_l \notin P\}. \end{aligned}$$

Note that for $x_i \in X$, if $v(x_i) = v(x_1)$, then we may let $x_i^* = x_i + \alpha_i x_1$ with $v(x_i^*) > v(x_1)$. Since the corresponding $m_i = 0$ then such a translation will not change the form of $\Pi x_i^{m_i} F(x_1, \dots, x_n)$ i. e., it will not affect the basic condition that $\Pi x_i^{m} \cdot F_d(x_1, \dots, x_n) \notin R^{p^e}$. So we may assume $v(x_i) > v(x_1)$ for all $x_i \in X$. Note that $F_d(x_1, \dots, x_n)$ is independent of x_l, $\forall x_l \notin Z$ because P is a permissible center.

Thus the monoidal transformation will be of the following form

$$\begin{aligned} x_1 &= \bar{x}_1 & & \\ x_i &= \bar{x}_1 \bar{x}_i & & \forall x_i \in X \\ x_j &= \bar{x}_1(\bar{x}_j + \alpha_j) & & \forall x_j \in Y \\ x_l &= \bar{x}_l & & \forall x_l \in Z \end{aligned}$$

where $0 \neq \alpha_j \in k$. For the following discussions we will introduce Hasse derivations $\{d_y^{(a)}\}$ as

Definition. *Let S be a commutative ring, $f(y)$ in $S[[y]]$ and $f(y+t) \in S[[y, t]]$. In the expansion*

$$f(y+t) = f(y) + \sum_{a \geq 1} f^{(a)}(y) t^a$$

the operation $d_y^{(a)}(f(y))$ is defined to be $f^{(a)}(y)$.

The following proposition is easy.

Proposition 1. *We have*

(1) *$d_y^{(1)}$ is the usual derivation and $d_y^{(a)}$ is linear over S.*

(2) *$f(y) \in S[[y^{p^r}]] \backslash S[[y^{p^r+1}]] \Leftrightarrow d_y^{(1)}(f(y)) = \dots = d_y^{(p^r-1)}(f(y)) = 0$ and $d_y^{(p^r)}(f(y)) \neq 0$.*

(3) *$d_y^{(p^r)}$ is a nonzero derivation on $S[[y^{p^r}]]$.*

Proof: We only prove (2), the rest being easy. Note that $d_y^{(j)}(y^s) = C_{s,j} y^{s-j}$ where $C_{s,j}$ is a binomial coefficient. For the part $\Rightarrow$, it follows from binomial expansion that $D_y^{(1)}(f(y)) = \dots = d^{(p^r-1)}(f(y)) = 0$. Let s be the minimal integer such that $a_s y^{sp^r}$ appears in $f(y)$ where $a_s \neq 0$ and $p \nmid s$. Then $d_y^{(p^r)}(a_s y^{sp^r}) = s a_s y^{(s-1)p^r} \neq 0$ and other terms are either zero or with exponents $> (s-1)p^r$. Thus $d_y^{(p^r)}(f(y)) \neq 0$. On the other hand, for the part $\Leftarrow$, let

$$f(y) \in S[[y^{p^{r_1}}]] \backslash S[[y^{p^{r_1+1}}]]$$

for some r_1. It is easy to see $r_1 = r$ by what we just proved.

Q. E. D.

Proposition 2. *Let k be a field of characteristic p, $y^m\varphi(y)\in k[y^{p^r}]\setminus k[y^{p^{r+1}}]$ and $0\neq\alpha\in k$. Let* deg $\varphi(y)=d^*$, $(y+\alpha)^m\varphi(y+\alpha)=\sum a_iy^i$, $c=\min\{i: a_i=0,\ p^{r+1}\nmid i\}$. *Then* $c\leq d^*+p^r$.

Proof: Let $\varphi(y)=y^n\cdot\varphi^*(y)$ with $\varphi^*(0)\neq 0$. Then we have $p^r|(m+n)$. Without losing gernality we may assume $n=0$, $p^r|m$, and $\varphi(y)\in k[y^{p^r}]$. It follows from our Proposition 1 that $d^{(p^r)}$ is a derivation on $k[y^{p^r}]$. Thus we get

$$d_y^{(p^r)}=d_{y+\alpha}^{(p^r)} \text{ on } k[y^{p^r}]$$

and

$$(y+\alpha)^{m-p^r},\ y^{c-p^r}\,|\,d_y^{(p^r)}((y+\alpha)^m\varphi(y+\alpha)).$$

Moreover, the right hand side is a polynomial of degree $\leq d^*+m-p^r$. Since $\alpha\neq 0$, $(y+\alpha)^{m-p^r}$ and y^{c-p^r} and are coprime. Then we have

$$m-p^r+c-p^r\leq d^*+m-p^r$$

or

$$c\leq d^*+p^r.$$

Q. E. D.

The blow-up with a permissible center P of $f(x_1,\dots,x_n)$ will transform $(\Pi x_i^{m_i})F(x_1,\dots,x_n)$ to the following

$$\bar{x}_1^{\bar{m}_1}\prod_{x_i\in X}\bar{x}_i^{m_i}\cdot\prod_{x_j\in Y}(\bar{x}_j+\alpha_j)^{m_j}\prod_{x_l\in Z}\bar{x}_l^{m_l}(F_d(1,\dots,\bar{x}_2,\dots,\bar{x}_j+\alpha_j,\dots,)+g)$$

where $\bar{m}_1=m_1+\sum_{x_i\in X}m_i+\sum_{x_j\in Y}m_j$ and $g\in I=$the ideal generated by $\{\bar{x}_1,\bar{x}_l: x_l\in Z\}$. Suppose $\bar{m}_1\not\equiv 0\,(p^e)$. Then in the product

$$\prod_{x_j\in Y}(\bar{x}_j+\alpha_j)^{m_j}.\ (F_d(1,\dots,\bar{x}_i,\dots,\bar{x}_j+\alpha_j,\dots)+g)$$

we consider the terms which do not involve $\bar{x}_1$ and $\bar{x}_l$ for all $x_l\in Z$. They will not be cancelled by terms in g and have order $\leq d$ in $\bar{x}_i$'s and $\bar{j}$'s.

Hence we may rewrite the transform of $\Pi x_i^{m_i}F(x_1,\dots,x_n)$ after throwing away p^e-th power terms as

$$\bar{x}_1^{\bar{m}_1}\prod_{x_i\in X}\bar{x}_i^{m_i}\prod_{x_l\in Z}\bar{x}_l^{m_l}(\tilde{F}_{\tilde{d}}(\bar{x}_1,\dots,\bar{x}_n)+\text{higher terms}).$$

Naturally we have $\tilde{d}\leq d$. Thus our stability theorem is proved in the case that $\bar{m}_1 \not\equiv 0 (p^e)$. For our convenience we shall call this case Possibility (I).

From now on, let us assume $\bar{m}_1 \equiv 0 (p^e)$. Due to our basic assumption that

$$\Pi x_i^{m_i} F_d(x_1, \ldots, x_n) \notin R^{p^e} = k[[x_1^{p^e}, \ldots, x_n^{p^e}]]$$

and $\bar{m}_1 \equiv 0 (p^e)$ it follows that

$$\begin{aligned} &\prod_{x_i \in X} \bar{x}_i^{m_i} \prod_{x_j \in Y} (\bar{x}_j + \alpha_j)^{m_j} \prod_{x_l \in Z} \bar{x}_l^{m_l} F_d(1, \ldots, \bar{x}_i, \ldots, \bar{x}_{j+d_j}, \ldots) \\ &\quad \notin k[\ldots, \bar{x}_i^{p^e}, \ldots, (\bar{x}_j + \alpha_j)^{p^e}, \ldots, \bar{x}_l^{p^e}, \ldots,] \\ &\quad = k[\bar{x}_2^{p^e}, \ldots, \bar{x}_i^{p^e}, \ldots, \bar{x}_j^{p^e}, \ldots, \bar{x}_l^{p^e}, \ldots]. \end{aligned}$$

So there is an $\bar{x}_s$ such that

$$\begin{aligned} &\Pi \bar{x}_i^{m_i} \Pi (\bar{x}_j + \alpha_j)^{m_j} \Pi \bar{x}_l^{m_l} F_d(1, \ldots, \bar{x}_i, \ldots, \bar{x}_j + \alpha_j, \ldots) \\ &\quad \notin k[\bar{x}_2, \ldots, \hat{\bar{x}}_s, \ldots, \bar{x}_j, \ldots][\bar{x}_s^{p^e}]. \end{aligned}$$

If $\bar{x}_s = \bar{x}_l$ for some $x_l \in Z$, i.e. $m_l \not\equiv 0 (p^e)$ then clearly the leading form of $\Pi \bar{x}_i^{m_i} \Pi (\bar{x}_j + \alpha_j)^{m_j} \Pi \bar{x}_l^{m_l} F_d$ coincides with $\Pi \bar{x}_i^{m_i} \Pi \bar{x}_l^{m_l}$ times the leading form of $(\Pi (\bar{x}_j + \alpha_j)^{m_j} F_d)$, which is not in $k[\bar{x}_2^{p^e}, \ldots, x_j^{p^e}, \ldots]$ and ord $\Pi (\bar{x}_j + \alpha_j)^{m_j} F_d(1, \ldots, \bar{x}_i, \ldots, \bar{x}_j + \alpha_j, \ldots) \leq d$. Thus our theorem is proved in this case. We shall call this case Possibility (II). Henceforth we may assume that $m_l \equiv 0 (p^e)$ for all $x_l \in Z$.

Let r be the nonnegative integer such that $\Pi x_i^{m_i} F_d(x_1, \ldots, x_n) \in R^{p^r} \backslash r^{p^{r+1}}$. Then clearly its transformation belongs to $(k[\bar{x}_1, \ldots, \bar{x}_n])^{p^r} \backslash (k[\bar{x}_1, \ldots, \bar{x}_n])^{p^{r+1}}$.

Note that $\Pi x_i^{m_i} F_d(x_1, \ldots, x_n) \in k[x_1^{p^r}, \ldots, x_n^{p^r}]$. If $p^r \nmid m_i$, then we may factor out more x_i from $F_d(x_1, \ldots, x_n)$. So, if necessary, we may assume that

$$p^r | d = \text{ord } F_d(x_1, \ldots, x_n).$$

Remark: In other words, ord $F_d(x_1, \ldots, x_n)$ may be taken to be less than or equal to $[d/p^r]p^r$ in the numerical discussions below.

We shall assume that for a particular $\bar{x}_s$

$$\begin{aligned} &\Pi \bar{x}_i^{m_i} \Pi (\bar{x}_j + \alpha_j)^{m_j} \Pi \bar{x}_l^{m_l} F_d(1, \ldots, \bar{x}_2, \ldots, \bar{x}_j + \alpha_j, \ldots) \\ &\quad \notin k[\bar{x}_2, \ldots, \hat{\bar{x}}_s, \ldots, \bar{x}_j, \ldots][\bar{x}_s^{p^{r+1}}]. \end{aligned}$$

For the remainder of the proof we will consider two possibilities;

(III) $\bar{x}_s \in X$ or (IV) $\bar{x}_s \in Y$.

Possibility (III): Note that

$$\Pi x_i^{m_i} \Pi x_j^{m_j} F_d(x_1, \ldots, x_i, \ldots, x_j, \ldots)$$
$$\notin k[x_1, \ldots, \hat{x}_s, \ldots, x_j, \ldots][x_s^{p^{r+1}}] \Leftrightarrow \Pi \bar{x}_i^{m_i} \Pi (\bar{x}_j+\alpha_j)^{m_j} F_d(1, \ldots,$$
$$\bar{x}_i, \ldots, \bar{x}_j+\alpha_j, \ldots) \notin k[\bar{x}_2, \ldots, \hat{\bar{x}}_s, \ldots, \bar{x}_j, \ldots][\bar{x}_s^{p^{r+1}}].$$

Let

$$\Pi \bar{x}_i^{m_i+n}(h(\{\bar{x}_j\}))$$

be a term in the expansion of $\Pi \bar{x}_i^{m_i} F_d(1, \ldots, \bar{x}_i, \ldots, \bar{x}_j+\alpha_j, \ldots)$ with $\bar{x}_i \in X$ as variables and $k[\{\bar{x}_j ; x_j \in Y\}]$ as coefficients. Note $p^{r+1} \nmid (m_s+n_s)$. Then clearly we have

$$\text{ord}\, h\, \Pi (\bar{x}_j+\alpha_j)^{m_i} \leq d - \sum n_i.$$

Thus we have established the non-increase of the order of F. Note that in all previous discussions the order of F will not increase.

Now let us recall Proposition 2 for the discussion of Possibility (IV). In the following expression let $\bar{y}_s = \bar{x}_s + \alpha_s$.

$$(\bar{x}_s+\alpha_a)^{m_s} F_d(1, \ldots, \bar{x}_i, \ldots, \bar{x}_j+\alpha_j, \ldots)$$
$$= \bar{y}_s^{m_s} F_d(1, \ldots, \bar{x}_i, \ldots, \bar{x}_j+\alpha_j, \bar{y}_s, \ldots)$$
$$= \sum \bar{y}_s^{m_s} g_I(\bar{y}_s) \Pi_{j \neq s} \bar{x}_j^{n_j}$$

where $I = (n_1, \ldots, n_j, \ldots)$ and $g_I(\bar{y}_s)$ is a polynomial in $\bar{y}_s$. We have at least one I such that

$$\bar{y}_s^{m_s} g_I(\bar{y}_s) \in k[\bar{y}_s^{p^r}] \backslash k[\bar{y}_s^{p^{r+1}}].$$

Say, $\bar{y}_s^{m_s} g_I(\bar{y}_s) \in k[\bar{y}^{p^r}] \backslash k[\bar{y}^{p^{r+1}}]$. Moreover we have

$$\deg g_I(\bar{y}_s) + |I| \leq d \ \text{(in fact, } [d/p^r]p^r. \text{ See Remark)}$$

where $|I| = \sum n_j$. Now make the substitution $\bar{y}_s = \bar{x}_s + \alpha_s$ and expand the polynomial. It follows from Proposition 2 that in the expansion there is a term $\bar{x}_s^c$ such that

$$p^{r+1} \nmid c,\ c \leq \deg g_I(\bar{y}_s) + p^r \leq d - |I| + p^r.$$

Moreover, it is easy to see that

(1) the total degree of $\bar{x}_x^c \cdot \Pi \bar{x}_j^{n_j}$ is at most $d + p^r$ (in fact, $[d/p^r] \cdot p^r + p^r$. See Remark.)

(2) $c \geq p^r$, $p^{r+1} \nmid c$.

Now we shall collect the polynomial in terms of $\bar{x}_s$ as follows :

$$(\bar{x}_s+\alpha_s)^{m_s}F_d(1,\dots,\bar{x}_j+\alpha_j,\dots)$$
$$=\sum h_i(\dots,\bar{x}_i,\dots,\bar{x}_j,\dots)\bar{x}_s^i.$$

Then we have by (1) that

(3) ord $h_c\bar{x}_s^c\leq d+p^r$ (in fact, $[d/p^r]p^r+p^r$. See Remark).

Now multiplying it with the remaining $(\bar{x}_j+\alpha_j)^{m_j}$, we conclude easily that

$$\text{ord}\prod_{j\neq s}(\bar{x}_j+\alpha_j)^{m_j}h_c\bar{x}_s^c\leq d+p^r.$$

Hence we have the following statement.

Statement: In the possibility (IV) after we blow-up the permissible center P, let ord $\tilde{F}=d_1$, then $\tilde{F}$ has a term A with

(i) ord $A\leq d+p^r$ (in fact, $[d/p^r]\cdot p^r+p^r$. See Remark)

(ii) $\text{ord}_{\bar{x}_s} A=c\geq p^r$ and $p^{r+1}\nmid c$

(iii) $d_1\leq\text{ord}\, A\leq d+p^r$ (in fact, $[d/p^r]p^r+p^r$. See Remark).

The interesting thing is that now $\bar{x}_s$ is an X-kind of variable due to the fact that m_s becomes zero. Furthermore, we shall use our Convention and call $\bar{x}_s$ the last variable.

Let us assume that $d_1=\text{ord}\, A=d+p^r$. We may request that c is the largest one satisfying conditions (i), (ii) and (iii) in the leading form of $\tilde{F}$. Let us examine the further blow-ups. There are two cases: (1) $v(\bar{x}_s)$ is the only minimal. (2) $v(\bar{x}_s)$ is not the only minimal. In the first case, we have to factor out $\bar{x}_s$ and do it without any translation. Due to the existence of the term A, the order of $\tilde{F}$ will drop at least by c which is $\geq p^r$. Hence the order of $\tilde{F}$ will drop to $d'\leq d$. Our proposition is proved in this case.

In the second case, we simply note that if by factoring out $\bar{x}_1$ (which is not $\bar{x}_s$) and then translating (i. e., replace $\bar{x}_s$ by $\bar{x}_1$ $(\bar{\bar{x}}_x+\alpha_s)$) the order of $\tilde{F}$ will not increase (c. f. Possibilities (I), (II) or (III)). If the order of $\tilde{F}$ drops by further blow-ups, we may assume that $d_1=\text{ord}\,\tilde{F}<[d/p^r]\cdot p^r+p^r$ from the very beginning.

Let us assume $d<d_1$. Then the following inequality

$$d<d_1<[d/p^r]p^r+p^r$$

implies

$$p^r \nmid d_1 .$$

Let r_1 be defined by

$$p^{r_1} | d_1$$
$$p^{r_1+1} \nmid d_1 .$$

Then $r_1 < r$. We conclude easily that the new bound for ord $\tilde{F}$ after blow-ups will be

$$d_1 + p^{r_1} < d + p^r.$$

Repeating the above argument, we establish that $d + p^r$ is the upper bound for orders for all successive blow-ups until the order becomes less than or equal to d. Q. E. D.

References

[AM1] S. S. ABHYANKAR AND T. T. MOH, Newton-Puiseux expansion and generalized Tschirnhausen transformation I, *Journal für die reine und angewandte Mathematik*, **260** (1973), 47-83.

[AM2] ———, Newton-Puiseux expansion and generalized Tschirnhausen transformation, II, *Journal für die reine und angewandte Mathematik*, **261** (1973), 29-53.

[H] H. HIRONAKA, Idealistic exponents of singularity, "*Algebraic Geometry*," Johns Hopkins Univ. Press, 1977.

[M] T. T. MOH, On two fundamental theorems for the concept of approximate roots, *J. Japan Math. Soc.*, **34**:4 (1982), 637-652.