Can. J. Math. Vol. **47** (4), 1995 pp. 801–816

A SIMPLE ALGORITHM FOR DECIDING PRIMES IN $K[[x,y]]$

TZEE-CHAR KUO

ABSTRACT. The well-known Tschirnhausen transformation, $x \longrightarrow x - \frac{a}{n}$, eliminates the second term of the polynomial $x^n + ax^{n-1} + \cdots$. By a mere repeated application of this transformation, one can decide whether a given element of $K[[x,y]]$ is prime (irreducible) or not. Here K is an algebraically closed field of characteristic 0.

A generalised version of Hensel's Lemma is developed for the proofs. The entire paper can be understood by undergraduate students.

1. Basics.

Semigroups. In this paper, by a semigroup we always mean an additive subsemigroup of the positive rationals, $\mathbb{Q}^+$. Also, we assume they are finitely generated. Thus, a semigroup, S, has a minimal set of generators, $\omega_0, \ldots, \omega_N$, and we write

$$S = S(\omega_0, \ldots, \omega_N),$$

where $0 < \omega_0 < \cdots < \omega_N$, and

$$\omega_i \notin S(\omega_0, \ldots, \omega_{i-1}), \quad i \geq 1.$$

A (finitely generated) semigroup is isomorphic to one whose generators are integers.

Let $d_0 = 1$ and let d_i denote the smallest integer such that

$$d_i\omega_i \in S(\omega_0, \ldots, \omega_{i-1}), \quad i \geq 1.$$

We may call $d_N\omega_N$ the *last merging point* of S.

Let $S_N = S(\omega_0, \ldots, \omega_N)$ be given. We write

$$\boldsymbol{\omega} = (\omega_0, \ldots, \omega_N);$$

a typical element of S_N can then be written as an "inner product"

$$M \cdot \boldsymbol{\omega} = \sum_{i=0}^{N} m_i\omega_i \tag{1}$$

where $M = (m_0, \ldots, m_N)$ in an $(N+1)$-tuple of non-negative integers.

We call M *admissible* if $0 \leq m_i < d_i$ for $1 \leq i \leq N$. (Note that $m_0 \geq 0$ can be any integer.)

Received by the editors December 27, 1993.

AMS subject classification: 13, 14, 32, 68.

DEFINITION. We say S_N is a Newton-Puiseux semigroup if $\omega_i > d_{i-1}\omega_{i-1}$ for all $i \geq 1$.

An element of a Newton-Puiseux semigroup S_N admits a unique expression (1), with M admissible. This is the Corollary to Lemma 2 in Section 6.

All semigroups arising in this paper are Newton-Puiseux.

Associated weight. Let S_N be given. Take indeterminants $Y_0, \ldots, Y_N$, and write

$$\mathbf{Y} = (Y_0, \ldots, Y_N), \quad \mathbf{Y}^M = Y_0^{m_0} \cdots Y_N^{m_N},$$

so that an element of the formal power series ring $K[[\mathbf{Y}]]$ is expressed as

$$f(\mathbf{Y}) = \sum_M a_M \mathbf{Y}^M, \quad a_M \in K.$$

Define a weight function on $K[[\mathbf{Y}]]$,

$$v_N : K[[\mathbf{Y}]] \longrightarrow \mathbb{Q}^+ \cup \{\infty\}$$

by

$$v_N(f) = \begin{cases} \min\{M \cdot \boldsymbol{\omega} \mid a_M \neq 0\}, & \text{if } f \neq 0, \\ \infty, & \text{if } f = 0. \end{cases}$$

Note that $v_N(Y_i) = \omega_i$.

We call $v_N(f)$ the *weighted order* of f associated to S_N.

Associated Newton polygon. Let S_N, v_N be as above.

Take an element in $K[[\mathbf{Y}, X]]$,

$$P(X; \mathbf{Y}) = \sum a_{M,d} \mathbf{Y}^M X^d, \quad a_{M,d} \in K.$$

In a coordinate plane, $\mathbb{R}^2$, let us plot a dot at the point $(d, M \cdot \boldsymbol{\omega})$ for each monomial term $a_{M,d}\mathbf{Y}^M X^d$, $a_{M,d} \neq 0$, of P. Note that the second component $M \cdot \boldsymbol{\omega}$ is an element of S_N. We call this dot a Newton dot.

When all M are admissible, there is at most one dot at a given point.

DEFINITION. The Newton polygon of $P(X; \mathbf{Y})$ associated to S_N is the boundary of the convex hull spanned by the set

$$\{(u, v) \mid \exists \text{ a Newton dot } (d, M \cdot \boldsymbol{\omega}) \text{ such that } u \geq d, v \geq M \cdot \boldsymbol{\omega}\}.$$

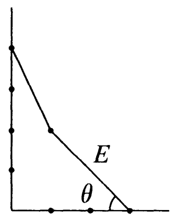
Suppose $P(X; \mathbf{Y})$ is regular in X, say of order k; that is,

$$P(X; 0) = X^k + \text{ higher order terms.}$$

Then, of course, $(k, 0)$ is a vertex of the Newton polygon. We call it the *first vertex*.

Let E denote the non-horizontal edge of the polygon at the first vertex, and θ the angle it makes with the negative horizontal direction, as indicated in the following example. We call E the *first edge*, and θ the *first angle*, of the Newton polygon of P, or simply of P.

EXAMPLE. $P(X, Y) = X^3 + XY^2 + Y^4$



G-adic bases. We follow Abhyankar-Moh ([1], [3]), who defined the notion.

Consider, as in [2], a sequence

$$\Gamma_N = \{G_0(x,y), \ldots, G_N(x,y), G_{N+1}(x,y)\}, \quad N \geq 0.$$

where $G_0 = y$, and for each $i \geq 1$, $G_i(x,y)$ is an element of $K[[y]][x]$, monic in x, say of degree D_i, such that each D_i properly divides D_{i+1}:

$$D_{i+1} = d_i D_i, \quad d_i > 1, \ 1 \leq i \leq N.$$

EXAMPLE. $\Gamma_1 = \{y, x, x^2 - y^3\}, \Gamma_2 = \{y, x, x^2 - y^3, (x^2 - y^3)^2 - xy^5\}$.

A repeated application of the Euclidean Division Algorithm shows that Γ_N is a G-adic base in the sense of Abhyankar-Moh ([1]): Given $F(x,y)$, there is a unique expression

$$F(x,y) = \sum a_{M,d} \mathbf{G}_N^M G_{N+1}^d \tag{2}$$

where $M = (m_0, \ldots, m_N)$ are admissible exponents, and $\mathbf{G}_N^M$ is a shorthand for $G_{\mathbf{0}}^{m_0} \cdots G_N^{m_N}$.

Let Γ_N be given a G-adic base. We define the *associated linear injection*

$$\ell_N : K[[x,y]] \longrightarrow K[[\mathbf{Y}, X]]$$

via (2) by:

$$\ell_N\big(F(x,y)\big) = \sum a_{M,d} \mathbf{Y}^M X^d. \tag{3}$$

Note that ℓ_N may not preserve multiplication. All exponents M in (3) are admissible. There is also an *associated substitution* map, which is a left inverse of ℓ_N,

$$\sigma_N : K[[\mathbf{Y}, X]] \longrightarrow K[[x,y]]$$

defined by

$$\sigma_N(Y_i) = G_i(x,y), \quad \sigma_N(X) = G_{N+1}(x,y),$$

preserving both the linear and multiplicative structures.

REMARK. When ℓ_N is given. A weighted order v_N is induced on $K[[x,y]]$ such that

$$v_N\big(F(x,y)\big) = v_n\Big(\ell_N\big(F(x,y)\big)\Big).$$

DEFINITION ([2]). When each G_i is a prime in $K[[x,y]]$, we say Γ_N is a Γ-adic base. All G-adic bases used in this paper are Γ-adic.

The Tschirnhausen transform. Let S_N, Γ_N and $P(X;\mathbf{Y})$ be given. Suppose P is in the image of ℓ_N, regular in X, of order k.

Suppose $\tan\theta \in S_N$, where θ is the first angle. We can write, as in (1),

$$\tan\theta = M\cdot\boldsymbol{\omega}, \quad M \text{ admissible.}$$

The *Tschirnhausen transform* of the pair (P,Γ_N) is defined as follows.

Consider the point $(k-1, M\cdot\boldsymbol{\omega})$, which lies on the first edge, E, next to the first vertex $(k,0)$. There is a Newton dot at this point if, and only if, P has a monomial term $a\mathbf{Y}^M X^{k-1}$, $a\neq 0$.

This dot can be eliminated by a Tschirnhausen transformation. Namely, we replace X by $X-\frac{a}{k}\mathbf{Y}^M$ in P to give

$$P'(X;\mathbf{Y}) = P\Big(X-\frac{a}{k}\mathbf{Y}^M;\mathbf{Y}\Big),$$

which no longer has a Newton dot at this point.

In the mean time, we replace G_{N+1} by

$$G^{(1)}_{N+1}(x,y) = G_{N+1}(x,y) + \frac{a}{k}\mathbf{G}^M_N. \tag{4}$$

Then, we define

$$\Gamma^{(1)}_N \equiv \{G_0,\ldots,G_N,G^{(1)}_{N+1}\},$$

and

$$P^{(1)}(X;\mathbf{Y}) = \ell_N\circ\sigma_N\big(P'(X;\mathbf{Y})\big).$$

The pair $\{P^{(1)},\Gamma^{(1)}_N\}$ is called the *Tschirnhausen transform* of $\{P,\Gamma_N\}$.

Observe that $(k,0)$ remains the first vertex of $P^{(1)}$; and also, clearly, $\theta^{(1)}\geq\theta$. (We use $\theta^{(1)}$ to denote the first angle of $P^{(1)}$.)

When $a=0$, the Tschirnhausen transformation is the identity transformation. We say it is *stationary*.

The following example shows that both cases $\theta^{(1)}>\theta$ and $\theta^{(1)}=\theta$ can happen. In either cases, however, there is no Newton dot at $(k-1,M\cdot\boldsymbol{\omega})$.

EXAMPLE. Take $\Gamma_0=\{y,x\}$. For $X^2+2XY+Y^2$, $\theta=\frac{\pi}{4}$, $\theta^{(1)}=\frac{\pi}{2}$. For $X^2+2XY+2Y^2$, $\theta^{(1)}=\theta=\frac{\pi}{4}$.

When $\tan\theta\notin S_N$, we say the transformation is *not applicable*. (Example: $\Gamma_0=\{y,x\}$, $P=x^2-y^3$.)

https://doi.org/10.4153/CJM-1995-041-9 Published online by Cambridge University Press

2. **The algorithm.** The Assertions in this section will be proved in later sections. Take a non-zero element of $K[[x,y]]$,

$$F(x,y) = H_k(x,y) + H_{k+1}(x,y) + \cdots,$$

where H_k is the initial (homogeneous) form.

By applying a suitable linear transformation, if necessary, we can assume $H_k(1,0) = 1$. An application of a Tschirnhausen transformation will then reduce H_k to

$$H_k(x,y) = x^k + a_2 x^{k-2} y^2 + \cdots + a_k y^k. \tag{5}$$

Let us describe the initial stage of the algorithm, assuming (5).

Take any $\omega_0 \in \mathbb{Q}^+$. (Indeed, we can take $\omega_0 = 1$.) Let $S_0 = S(\omega_0)$, and let v_0 be defined by $v_0(Y_0) = \omega_0$. Take the first Γ-adic base to be

$$\Gamma_0 = \{G_0 = y, G_1 = x\}.$$

The associated maps ℓ_0, σ_0 are defined accordingly. Finally, let

$$P_0(X; Y_0) = \ell_0\big(F(x,y)\big),$$

which is regular in X, of order $k_0 = k$.

Now assume, inductively, that we are at stage N, $N \geq 0$, having defined a Newton-Puiseux semigroup, $S_N = S(\omega_0, \ldots, \omega_N)$, a Γ-adic base Γ_N, together with v_N, ℓ_N, σ_N, and

$$P_N(X; \mathbf{Y}) = \ell_N\big(F(x,y)\big), \quad \mathbf{Y} = (Y_0, \ldots, Y_N).$$

where P_N is regular in X, say, of order k_N.

ASSERTION 1. If $k_N = 1$, then $F(x,y)$ is prime.

In case $k_N > 1$, we apply the Tschirnhausen transformation recursively to the pair $\{P_N, \Gamma_N\}$, as long as it is applicable. This yields a sequence $\{P_N^{(s)}, \Gamma_N^{(s)}\}$, where $P_N^{(0)} = P_N$, $\Gamma_N^{(0)} = \Gamma_N$, and $\{P_N^{(s)}, \Gamma_N^{(s)}\}$ is the Tschirnhausen transform of $\{P_N^{(s-1)}, \Gamma_N^{(s-1)}\}$, for all s. Four cases may arise:

CASE 1. The transformation is always applicable, yielding an infinite sequence $\{P_N^{(s)}, \Gamma_N^{(s)}\}$.

CASE 2. We arrive at $\{P_N^{(s)}, \Gamma_N^{(s)}\}$, and find $\tan\theta_N^{(s)} = \infty$. (Here, $\theta_N^{(s)}$ denotes the first angle of $P_N^{(s)}$.)

CASE 3. Or, here we find that the Tschirnhausen transformation is stationary, with

$$\tan\theta_N^{(s)} \in S_N, \quad (\tan\theta_N^{(s)} < \infty).$$

CASE 4. Or, we have, $\tan\theta_N^{(s)} \notin S_N$, (so that it is no longer applicable).

ASSERTION 2. $\Gamma_N^{(s)}$ are Γ-adic bases.

ASSERTION 3. In Cases 1 and 2, ($k_N > 1$), $F(x,y)$ is the k-th power of a prime, hence reducible.

ASSERTION 4. In Case 3, $F(x,y)$ is reducible.

When Case 4 happens, we move on to define the $(N+1)$-st stage. Let $w_{N+1} = \tan \theta_N^{(s)}$, $S_{N+1} = S(w_0, \ldots, w_{N+1})$, and let d_{N+1} be the smallest integer such that

$$d_{N+1}\omega_{N+1} \in S_N, \quad (d_{N+1} > 1).$$

We shall see, in Section 4, that S_{N+1} is Newton-Puiseux.

When k_N is divisible by d_{N+1}, we define k_{N+1} and an admissible exponent $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_N)$ by

$$k_N = k_{N+1}d_{N+1}, \quad \boldsymbol{\alpha} \cdot \boldsymbol{\omega} = d_{N+1}\omega_{N+1}.$$

ASSERTION 6. Consider the monomial term, $a\mathbf{Y}^\alpha X^{k_N - d_{N+1}}$ of $P_N^{(s)}$. If $a = 0$, then $F(x,y)$ is reducible.

Now, suppose $a \neq 0$. We define

$$G_{N+2} = G_{N+1}^{(s)} + \frac{a}{k_{N+1}}\mathbf{G}_N^\alpha, \qquad (6)$$
$$\Gamma_{N+1} = \{G_0, \ldots, G_{N+1}^{(s)}, G_{N+2}\},$$

and

$$P_{N+1}(X; \mathbf{Y}_{N+1}) = \ell_N\big(F(x,y)\big)$$

which is regular in X, of order k_{N+1}, where

$$\ell_{N+1}(G_{N+1}) = Y_{N+1}, \quad \mathbf{Y}_{N+1} = (Y_0, \ldots, Y_{N+1}).$$

ASSERTION 7. G_{N+1} is prime, whence Γ_{N+1} is a Γ-adic base.

This completes the description of the algorithm.

Since $\{k_N\}$ is a strictly decreasing sequence of positive integers, Case 4 can not happen infinitely many times. The algorithm terminates in finitely many steps.

ATTENTION. Since G_{N+1} has been replaced by $G_{N+1}^{(s)}$ when G_{N+2} is defined, Γ_N is not necessarily a subset of Γ_{N+1}. However, note that

$$G_{N+1}^{(s)} = G_{N+1} + \text{ terms of higher weight.}$$

CONVENTION. When Γ_{N+1} has been defined. We shall use Γ_N to denote $\Gamma_N^{(s)}$, abusing notations, and then forget about the original Γ_N. In this new system of notations, Γ_N is a subset of Γ_{N+1}, for all N.

3. **Illustrative examples.** A simple example for Case 1 is:

$$x^2 + 2xy^2 + 2xy^3 + y^4 + 2xy^4 + 2y^5 + \cdots = (x + y^2 + y^3 + y^4 + \cdots)^2.$$

For Case 2, we can take

$$(x^2 + 2xy + y^2) + (xy^2 + y^3) + \frac{1}{4}y^4 = \left[(x+y) + \frac{1}{2}y^2\right]^2.$$

For Case 3, consider

$$F = (x^2 - y^3)^2 - y^7.$$

Here, we find

$$\begin{aligned} \nu(x) &= \nu(G_1) = 3/2, \\ S_1 &= S(1, 3/2), \\ G_2 &= x^2 - y^3, \\ P_1 &= X^2 - Y^7, \\ \tan\theta_1 &= 7/2 \in S_1. \end{aligned}$$

The Tschirnhausen transformation is stationary, F is reducible by Assertion 4. (The term $G_1 Y^2$ is missing from P_1.) A factorization is given at the end of Section 8.

For Case 4, our first example is $F = x^3 - xy^3 + y^5$. Here we have,

$$\begin{aligned} N &= 0, \\ P_0 &= X^3 - XY^3, \\ k_0 &= 3, \\ d_1 &= 2. \end{aligned}$$

Since k_0 is not divisible by d_1, F is reducible (Assertion 5).

Next, consider

$$F = (x^2 - y^3)^4 + y^{13}.$$

Here, we find

$$\begin{aligned} N &= 1, \\ G_1 &= x, \\ G_2 &= x^2 - y^3, \\ P_1 &= X^4 + Y^{13}, \\ \tan\theta_1 &= 3\frac{1}{4}, \\ d_1 &= 2. \end{aligned}$$

By Assertion 6, F is reducible. (The term $G_1 Y^5$ is missing from P_1.)

https://doi.org/10.4153/CJM-1995-041-9 Published online by Cambridge University Press

Now let us consider

$$F = (x^2 - y^3)^4 + 2xy^5(x^2 - y^3)^2 + 2y^{13} + \cdots .$$

Here,

$$P_1 = X^4 + 2G_1Y^5X^2 + 2Y^{13}.$$

Following the algorithm, we define

$$G_3 = (x^2 - y^3)^2 + xy^5$$

which, by Assertion 7, is prime.

Finally, let us consider

$$(x^2 - y^3)^4 + 2xy^5(x^2 - y^3)^2 + y^{13} + \text{ higher weighted terms.}$$

This time,

$$\begin{aligned} P_1 &= X^4 + 2G_1Y^5X^2 + Y^{13} \\ &= (X^2 + G_1Y^5)^2 + \cdots , \end{aligned}$$

so that we move on to the next stage of the algorithm.

4. **Induction hypothesis.** We make two induction hypothesis at Stage N; they will be proved for $N+1$ at the end of Section 9.

(H_P) For the first angle θ_N of P_N, we have

$$\tan \theta_N \geq d_N\omega_N,$$

and if equality holds then there is no Newton dot at $(k_N - 1, \tan\theta_N)$.

(H_G) For $N \geq 1$, $G_{N+1}(x,y)$ has the form

$$G_{N+1} = G_N^{d_N} + c\mathbf{G}_{N-1}^{\boldsymbol{\alpha}_{N-1}}, \quad c \neq 0,$$

where $\boldsymbol{\alpha}_{N-1} = (\alpha_0, \ldots, \alpha_{N-1})$ is an admissible exponent such that

$$\sum_{i=0}^{N-1} \alpha_i\omega_i = d_N\omega_N.$$

When $N = 0$, (H_P) follows from (5); (H_G) says nothing, hence true.

5. **Stage $N = 0$.** We can assume $\omega_0 = 1$.

If $k = k_0 = 1$, $F(x,y)$ is obviously prime. So let us suppose $k > 1$.

In Case 1, where the Tschirnhausen transformation is always applicable, we find an infinite series $\sum C_ny^n$ such that

$$F(x,y) = \left(x - \sum C_ny^n\right)^k \cdot \text{unit}.$$

In Case 2, there is a finite series with the same property.

https://doi.org/10.4153/CJM-1995-041-9 Published online by Cambridge University Press

Therefore Assertions 2 and 3 are true when $N = 0$.

For Assertion 4, let us first assume $\tan\theta_0 = 1$. By (5), the initial form of $P_0(X; Y)$ has the form

$$I(X, Y) = X^k + a_2X^{k-2}Y^2 + \cdots + a_kY^k.$$

Since at least one $a_i \neq 0$, $I(X, 1) = 0$ has at least two distinct roots, and so $I(X, Y)$ factors:

$$I(X, Y) = H_p(X, Y) \cdot K_q(X, Y), \quad p + q = k,$$

H_p, K_q are relatively prime (homogeneous) forms of degree p, q respectively, both monic in X.

LEMMA 1. *Every $(p + q - 1)$-form $L_{p+q-1}(X, Y)$ is in the ideal generated by H_p and K_q. That is, there exist forms A_{p-1}, B_{q-1} such that*

$$L_{p+q-1}(X, Y) = B_{q-1}(X, Y)H_p(X, Y) + A_{p-1}(X, Y)K_q(X, Y). \tag{7}$$

Consequently, every r-form, $r \geq p + q - 1$, is in this ideal.

The proof is well-known. Since H_p, K_q are relatively prime, polynomials A_{p-1}, B_{q-1}, of degree $p - 1, q - 1$, respectively, can be found such that

$$L_{p+q-1}(X, 1) = B_{q-1}(X)H_p(X, 1) + A_{p-1}(X)K_q(X, 1).$$

Then (7) follows by homogenizing this expression.

Now, consider any power series $P(X, Y)$, such as $P_0(X, Y)$, whose initial form is $I(X, Y)$. By a repeated application of Lemma 1, we can recursively find forms A_i, B_i such that

$$P(X, Y) = [H_p + A_{p+1} + A_{p+2} + \cdots][K_q + B_{q+1} + B_{q+2} + \cdots].$$

An application of σ_0 to $P_0(X, Y)$ then yields a factorization of $F(x, y)$.

Now, suppose $\tan\theta_0 > 1$ in Case 3. Let us define weights by

$$\nu(X) = \tan\theta_0, \quad \nu(Y) = 1.$$

Since there is no Newton dot at $(k - 1, \tan\theta_0)$, the weighted initial form of $P_0(X, Y)$ factors into two relatively prime weighted forms. The same reasoning as before will then lead to a factorization of P_0.

This is known as the weighted Hensel Lemma.

We shall consider stage $N = 0$ of Case 4 with the general case.

6. **More on Newton-Puiseux semigroups.** Consider a (finitely generated) semigroup S_N. The abelian group generated by S_N is generated by a single element, say g. There is a smallest integer r such that $(r + i)g \in S_N$ for all $i \geq 0$. Call rg the *conductor* of S_N.

When a semigroup is generated by two positive integers p, q, the conductor is $(p' - 1)(q' - 1)D$, where

$$D = \text{G.C.D.}(p, q), \quad p = p'D, \quad q = q'D.$$

When there are more than two generators, there is no simple formula for calculating the conductor. However, by an easy induction on N we can prove the following

LEMMA 2. *In a Newton-Puiseux semigroup S_N, the conductor is $\leq d_N\omega_N$. (Thus, beyond the last merging point, S_N coincides with the abelian group it generates).*

COROLLARY. *Every element in S_N admits a unique expression (1) with M admissible.*

PROOF. Suppose M, M' are admissible and $M \cdot \boldsymbol{\omega} = M' \cdot \boldsymbol{\omega}$, $m_N > m'_N$. Then $(m_N - m'_N)\omega_N$ belongs to the abelian group generated by S_{N-1}, hence to S_{N-1} itself. This is absurd, hence $m_N = m'_N$. Similarly, $m_i = m'_i$ for all other i.

7. **Construction of primes.** We are in stage N, having defined S_N, Γ_N, *etc.* The induction hypothesis H_P and H_G are also at our disposal.

Take any rational number $\omega_{N+1} \geq d_N\omega_N$. Let d_{N+1} denote the smallest integer such that

$$d_{N+1}\omega_{N+1} \in S_N, \quad (d_{N+1} = 1 \text{ if } \omega_{N+1} \in S_N).$$

Let $\boldsymbol{\alpha} = (\alpha_0, \dots, \alpha_N)$ be the admissible exponent such that

$$\boldsymbol{\alpha} \cdot \boldsymbol{\omega} = d_{N+1}\omega_{N+1} \tag{8}$$

Take an integer $r \geq 2$. Note that $r\boldsymbol{\alpha} = (r\alpha_0, \dots, r\alpha_N)$ may not be admissible. When this happens, we like to investigate the expansion (3) for $\mathbf{G}_N^{r\boldsymbol{\alpha}}$.

For this purpose, it is convenient to define a weight on X and G_{N+1}:

$$v(X) = v(G_{N+1}) = \omega_{N+1}. \tag{9}$$

LEMMA 3. *Let $E = (e_0, \dots, e_n)$ be a given exponent.*

(i) Suppose $\omega_{N+1} > d_N\omega_N$. Then the weighted initial form of $\ell_N(\mathbf{G}_N^E)$ consists of only one monomial term $a\mathbf{Y}^\beta$, where $a \neq 0$, $\boldsymbol{\beta}$ is admissible, and

$$\boldsymbol{\beta} \cdot \boldsymbol{\omega} = E \cdot \boldsymbol{\omega}.$$

(ii) Suppose $\omega_{N+1} = d_N\omega_N$, and suppose $e_N < d_N$. Then the same is true.

(iii) Suppose $\omega_{N+1} = d_N\omega_N$. Then $\alpha_N = 0$. Hence if $E = r\boldsymbol{\alpha}$, again the same is true.

EXAMPLE. Consider $\Gamma_1 = \{y, x, x^2 - 2y^3\}$. Here $\omega_1 = 3/2$.
Let us compute the expansion of $(yx)^2$:

$$(yx)^2 = y^2[(x^2 - 2y^3) + 2y^3] = 2y^5 + y^2(x^2 - 2y^3).$$

In case we take $\omega_2 > d_1\omega_1 = 3$, $2y^5$ has the lowest weight,

$$v(2y^5) = 5 < v\big(y^2(x^2 - 2y^3)\big),$$

confirming (i).

However, if we take $\omega_2 = 3$, then both terms have weight 5; this explains why we assume $e_N < d_N$ in (ii).

PROOF. For an admissible exponent, E, there is nothing to prove.

Define an ordering of the exponents as follows:

$$(e'_0, \ldots, e'_N) < (e_0, \ldots, e_N)$$

if $\exists j$, $e'_j < e_j$ and $e'_i = e_i$ $\forall i > j$.

Now, suppose E is not admissible. Let $j > 0$ be the largest integer such that $e_j \geq d_j$. By (H_G), we can write

$$G_j^{d_j} = -c\mathbf{G}_{j-1}^{\alpha_{j-1}} + G_{j+1}. \tag{10}$$

Note that the first two terms both have weight $d_j\omega_j$; the third term, G_{j+1}, has higher weight for all j, $1 \leq j \leq N$, in case (i). In case (ii), this is true for all j, $1 \leq j \leq N-1$.

By a repeated application of (10), it follows that there is an exponent $E' < E$, such that

$$\mathbf{G}_N^E = C^*\mathbf{G}_N^{E'} + \text{ higher weighted terms},$$

where $C^* \neq 0$, $E \cdot \boldsymbol{\omega} = E' \cdot \boldsymbol{\omega}$.

Take an E' with this property which is minimal in the ordering. This E' must be admissible.

The proof of (iii) is easy. Since $d_N\omega_N \in S_{N-1}$, and $\boldsymbol{\alpha}$ is admissible, we must have $\alpha_N = 0$.

We introduce a terminology. Let g be the generator of the abelian group generated by S_N. Given an integer m, let $\mathcal{M}_{mg}$ denote the ideal in $K[[\mathbf{Y}, X]]$ of elements with weighted order $\geq mg$.

Given $P(X;\mathbf{Y})$, $P'(X;\mathbf{Y})$ in $\mathcal{M}_{mg}$, we say they are congruent modulo higher weighted terms, if

$$\ell_N \circ \sigma_N(P - P') \in \mathcal{M}_{(m+1)g}.$$

When $\mathcal{M}_{mg}$ is understood, we simply write

$$P(X;\mathbf{Y}) \equiv P'(X;\mathbf{Y}) \text{ m. h. w. t.}$$

Let $f(x,y) = \sigma_N(P)$, $f'(x,y) = \sigma_N(P')$; we also write

$$f(x,y) \equiv f'(x,y) \text{ m. h. w. t.}$$

Recall that ℓ_N may not preserve multiplication. However, we shall show it preserves the weighted initial form modulo higher weighted terms in the following sense.

Again, let us take any $\omega_{N+1} \geq d_N\omega_N$, and defined weights as in (9). Then the weighted initial form of a given $P(X;\mathbf{Y})$ is defined.

Let $F_i(x,y)$, $i = 1, 2, 3$, be given with

$$F_3(x,y) = F_1(x,y)F_2(x,y).$$

LEMMA 4. *Let $W_i(X;\mathbf{Y})$ denote the weighted initial form of $\ell_N(F_i)$. Then*

$$W_1(X;\mathbf{Y})W_2(X;\mathbf{Y}) \equiv W_3(X;\mathbf{Y}) \text{ m. h. w. t.}$$

PROOF. Recall that σ_N preserves multiplication. Hence

$$\ell_N \circ \sigma_N\big(\ell_N(F_1)\ell_N(F_2)\big) = \ell_N(F_3). \tag{11}$$

Consider a typical term in $\ell_N(F_1)\ell_N(F_2)$,

$$\xi \equiv C_1 C_2 \mathbf{Y}^{E_1+E_2} X^{d_1+d_2},$$

where $C_1 \mathbf{Y}^{E_i} X^{d_i}$ is a monomial term in $\ell_N(F_i)$.

By Lemma 3, $\ell_N \circ \sigma_N(\xi)$ has the same weighted order as ξ.

Now, comparing terms of minimal weighted order on both sides of (11), we find

$$\ell_N \circ \sigma_N(W_1 \cdot W_2) \equiv W_3 \text{ m. h. w. t.}$$

Several important consequences can be derived from this lemma. First, let us take $\omega_{N+1} = d_N \omega_N$. Let $H(G_0, \ldots, G_{N+1})$ be any series with weighted order $> \omega_{N+1}$.

LEMMA 5. *$G_{N+1} + H(G_0, \ldots, G_{N+1})$ is prime.*

This is clear: $\ell_N(G_{N+1} + H)$ has weighted initial form X, which is irreducible.

EXAMPLE. Consider $\Gamma_1 = \{y, x, x^2 - y^3\}$. Here, $G_2 + y^3 = x^2$ is not prime. Note that $v(y^3) = \omega_2$, and hence Lemma 5 does not apply.

Using the inductive hypothesis (H_P), we see that $G_{N+1}^{(i)}$, $i \geq 0$, are all primes.

Assertion 1 follows. Indeed, when $k_N = 1$, there is a finite, or infinite, series H, such that

$$F(x, y) = (G_{N+1} + H) \cdot \text{unit}.$$

Assertions 2 and 3 are immediate consequences too.

Now, let us take $\omega_{N+1} \notin S_N$, $\omega_{N+1} > d_N \omega_N$, and $\boldsymbol{\alpha}$ satisfying (8). Take a constant $c \neq 0$.

LEMMA 6. *Let $H(G_0, \ldots, G_{N+1})$ be a series with weighted order $> d_{N+1}\omega_{N+1}$. Then*

$$G_{N+1}^{d_{N+1}} - c\mathbf{G}_N^{\boldsymbol{\alpha}} + H(G_0, \ldots, G_{N+1})$$

is a prime.

The corresponding weighted initial form is $X^{d_{N+1}} - c\mathbf{Y}^{\boldsymbol{\alpha}}$, having weight $d_{N+1}\omega_{N+1}$. It has to be irreducible, since any weighted form of lower weighted form of lower weight consists of at most one monomial, and the product of two such is a single monomial term.

8. **Proof of Assertion 4** ($N \geq 1$). We are at stage N, having defined P_N, θ_N, *etc.* and then, being in Case 3, arrived at $P_N^{(s)}$, $\theta_N^{(s)}$. We shall write $P_N^{(s)}$, $\theta_N^{(s)}$ as P_N, θ_N, for simplicity of notation.

Let $\boldsymbol{\alpha}$ denote the admissible exponent such that $\boldsymbol{\alpha} \cdot \boldsymbol{\omega} = \tan\theta_N\big(= v(X)\big)$. Take a Newton dot on the first edge, representing a term of P_N of the form

$$a_r \mathbf{Y}^E X^{k_N - r}, \quad a_r \neq 0.$$

Then Lemma 3 can be applied to $r\boldsymbol{\alpha}$, giving a constant $c_r \neq 0$ such that

$$a_r \mathbf{Y}^E \equiv c_r \mathbf{Y}^{r\boldsymbol{\alpha}} \text{ m. h. w. t.}$$

These c_r can be used to define a homogeneous form in two variables

$$W(X, Y) = X^{k_N} + c_2 X^{k_N - 2} Y^2 + \cdots.$$

Attention should be paid to the absence of c_1; this is because we are in Case 3, there is no Newton dot at the corresponding point.

Observe that

$$W(X, \mathbf{Y}^{\boldsymbol{\alpha}}) \equiv P_N(X; \mathbf{Y}) \text{ m. h. w. t.}$$

Hence we can consider $W(X, \mathbf{Y}^{\boldsymbol{\alpha}})$, as the weighted initial form of P_N.

Since at least one $c_r \neq 0$, $(r > 1)$, $W(X, Y)$ factors:

$$W(X, Y) = H_p(X, Y) K_q(X, Y), \quad p + q = k_N, \tag{12}$$

where H_p, K_q are relatively prime homogeneous forms, monic in X.

Take any monomial $\mathbf{Y}^E X^d$ with weight

$$E \cdot \boldsymbol{\omega} + d \tan\theta_N > k_N \tan\theta_N.$$

Choose an integer $j \geq 0$ and a rational number t such that

$$E \cdot \boldsymbol{\omega} = j \tan\theta_N + t, \quad 0 \leq t < \tan\theta_N.$$

By Lemma 2, there is an admissible exponent J such that

$$\tan\theta_N + t = J \cdot \boldsymbol{\omega}.$$

Let us first consider the case

$$E \cdot \boldsymbol{\omega} \geq \tan\theta_N \quad (\text{hence } j \geq 1).$$

By Lemma 3, there exists a constant $C^* \neq 0$ such that

$$\mathbf{Y}^E \equiv C^* \mathbf{Y}^J \mathbf{Y}^{(j-1)\boldsymbol{\alpha}} \text{ m. h. w. t.}$$

Since $d + j = k_N$, Lemma 1 can be applied to $Y^{j-1} X^{d^*}$, for (12), giving

$$Y^{j-1} X^d = B_{s-p}(X, Y) H_p(X, Y) + A_{s-q}(X, Y) K_q(X, Y)$$

https://doi.org/10.4153/CJM-1995-041-9 Published online by Cambridge University Press

where $s = d + j - 1$.

On substituting Y by $\mathbf{Y}^{\boldsymbol{\alpha}}$, we find that $\mathbf{Y}^E X^d$ is in the ideal generated by $H_p(X, \mathbf{Y}^{\boldsymbol{\alpha}})$, $K_q(X, \mathbf{Y}^{\boldsymbol{\alpha}})$, modulo higher weighted terms.

Now, consider the case

$$E \cdot \boldsymbol{\omega} < \tan\theta_N.$$

In this case, $j = 0$ and hence $d \geq 1$. Lemma 1 applies to X^{d-1}. Again, $\mathbf{Y}^E X^d$ is in the ideal generated by $H_p(X, \mathbf{Y}^{\boldsymbol{\alpha}})$, $K_q(X, \mathbf{Y}^{\boldsymbol{\alpha}})$.

The rest of the argument is standard for Hensel's Lemma. We can recursively find weighted forms A', B', A'', B'', *etc.* with increasing weights, such that

$$[H_p + A' + A'' + \cdots][K_q + B' + B'' + \cdots]$$

has $F(x, y)$ as its image under σ_N. Thus $F(x, y)$ is reducible, proving Assertion 4.

EXAMPLE.

$$(x^2 - y^3)^2 - y^7 = \left[(x^2 - y^3 + xy^2) + \frac{1}{2}y^4 + \frac{1}{4}xy^3 + \cdots\right] \cdot \left[(x^2 - y^3 - xy^2) + \frac{1}{2}y^4 - \frac{1}{4}xy^3 + \cdots\right].$$

9. **Proofs of Assertions 5 to 7.** We are in Case 4. Define $v(X) = \omega_{N+1}$ and let $\boldsymbol{\alpha}$ be an admissible exponent satisfying (8).

By an argument similar to that in Section 8, we can define

$$W(X, Y) = X^{k_N} + C_1 X^{k_N - d_{N+1}} Y + C_2 X^{k_N - 2d_{N+1}} Y^2 + \cdots$$

such that

$$W(X, \mathbf{Y}^{\boldsymbol{\alpha}}) \equiv P_N(X; \mathbf{Y}) \text{ m. h. w. t.}$$

Now, suppose k_N is not divisible by d_{N+1}. Let k_N be divided by d_{N+1}:

$$k_N = Q d_{N+1} + R, \quad 0 < R < d_{N+1}, \tag{13}$$

so that

$$W(X, Y) = X^R H(\xi, \eta),$$

where

$$\xi \equiv X^{d_{N+1}}, \quad \eta \equiv Y,$$

and $H(\xi, \eta)$ is a homogeneous Q-form, monic in ξ. The equation $H(\xi, 1) = 0$ may, or may not, have $\xi = 0$ as a root. Let $\mu \geq 0$ denote the multiplicity.

First, assume $\mu = 0$.

Let $I\big(\xi, H(\xi, \eta)\big)$ denote the ideal generated by ξ and $H(\xi, \eta)$. Then, clearly.

$$\eta^Q \in I\big(\xi, H(\xi, \eta)\big). \tag{14}$$

Take a monomial $\mathbf{Y}^E X^d$ such that

$$E \cdot \boldsymbol{\omega} + d\omega_{N+1} > k_N \omega_{N+1}. \tag{15}$$

We claim that

$$\mathbf{Y}^E X^d \in I\big(X^R, H(X^{d_{N+1}}, \mathbf{Y}^{\boldsymbol{\alpha}})\big). \tag{16}$$

This is obvious if $d \geq R$. In case $d < R$, it suffices to show that $\mathbf{Y}^E$ is divisible by $\mathbf{Y}^{Q\boldsymbol{\alpha}}$. Then (16) follows from (14).

By (13),

$$E \cdot \boldsymbol{\omega} - Qd_{N+1}\omega_{N+1} > (R - d)\omega_{N+1} \geq d_N \omega_N.$$

Hence the left-hand side, being an element of the abelian group generated by S_N, is actually in S_N, by Lemma 2. There is an exponent E^* such that

$$E \cdot \boldsymbol{\omega} = E^* \cdot \omega + Qd_{N+1}\omega_{N+1},$$

whence

$$\mathbf{Y}^E = \mathbf{Y}^{E^*}(\mathbf{Y}^{\boldsymbol{\alpha}})^Q.$$

Now, suppose $\mu \geq 1$. Let us write

$$H(\xi, \eta) = \xi^\mu K(\xi, \eta), \quad K(0, 1) \neq 0.$$

Lemma 1 is applicable to the pair ξ^μ, $K(\xi, \eta)$, so that

$$\xi^{i-1}\eta^{Q-i} \in I\big(\xi^\mu, K(\xi, \eta)\big), \quad 1 \leq i \leq Q. \tag{17}$$

Take a monomial $\mathbf{Y}^E X^d$ with property (15). We claim that

$$\mathbf{Y}^E X^d \in I\big(X^{\mu d_{N+1}+R}, K(X^{d_{N+1}}, \mathbf{Y}^{\boldsymbol{\alpha}})\big). \tag{18}$$

In case $d \geq \mu d_{N+1} + R$, this is obvious. Otherwise, let μ' denote the largest integer such that

$$(\mu' - 1)d_{N+1} + R \leq d < \mu' d_{N+1} + R.$$

Then, by a similar argument, we can show that $\mathbf{Y}^E X^d$ is divisible by

$$X^{(\mu'-1)d_{N+1}+R}\mathbf{Y}^{(Q-\mu')\boldsymbol{\alpha}}.$$

Hence (18) follows from (17).

Both for $\mu = 0$ and for $\mu > 0$, we can now use an argument similar to that for Assertion 4 to conclude that $F(x, y)$ is reducible, proving Assertion 5.

Finally, let us assume k_N is divisible by d_{N+1}, so that $R = 0$ in (13).

Coefficient $C_1, C_2, \ldots,$ can be determined so that

$$W(\xi, Y) = \xi^Q + C_1\xi^{Q-1}Y + \cdots + C_Q Y^Q$$

has the property that

$$W(X^{d_{N+1}}, \mathbf{Y}^{\boldsymbol{\alpha}}) \equiv P_N(X; \mathbf{Y}) \text{ m. h. w. t.}$$

Suppose $C_1 = 0$. Since at least one other $C_i \neq 0$, $W(\xi, Y)$ factors into two relatively prime factors, monic in ξ. Let us consider

$$\{G_0, \ldots, G_{N+1}, G_{N+2}\}, \quad G_{N+2} = G_{N+1}^{d_{N+1}}.$$

This is G-adic base, but not a Γ-adic base. Consider the expansion (3) of $F(x,y)$ with respect to this base. Since $W(\xi, Y)$ factors, by repeating the argument for Assertion 4, we come to the conclusion that $F(x,y)$ is reducible. This completes the proof of Assertion 6.

Now assume $C_1 \neq 0$. Define

$$G_{N+2} = G_{N+1}^{d_{N+1}} + \frac{C_1}{Q} \mathbf{G}_N^{\boldsymbol{\alpha}},$$

which, by Lemma 6, is prime, proving Assertion 7.

Note that the induction hypothesis (H_G) has also been proved for $N+1$.

As for (H_P), using $\Gamma_{N+1} = \{G_0, \ldots, G_{N+2}\}$ as the Γ-adic base, $P_{N+1}(X; Y_0, \ldots, Y_{N+1})$ is defined, having first vertex at $(k_{N+1}, 0)$.

In case

$$W(\xi, 1) = \left(\xi + \frac{C_1}{Q}\right)^Q \tag{19}$$

we clearly have

$$\tan \theta_{N+1} > d_{N+1} \omega_{N+1}.$$

In case (19) does not hold, we will have

$$\tan \theta_{N+1} = d_{N+1} \omega_{N+1},$$

but there will be no Newton dot at $(k_{N+1} - 1, \tan \theta_{N+1})$.

ACKNOWLEDGMENT. The author would like to thank his son, Dean, and Scot McCullum, for many valuable communications related to the Computer Science aspects of this result.

REFERENCES

1. S. Abhyankar and T. T. Moh, *Newton-Puiseux expansion and generalised Tschirnhausen transformation I, II*, J. Reine Angew. Math. **260**(1973), 47–83; *ibid.* **261**(1973), 29–54.

2. T.-C. Kuo, *Generalised Newton-Puiseux theory and Hensel's lemma in* C[[x,y]], Canad. J. Math. (6) **XLI**(1989), 1101–1116.

3. T. T. Moh, *On the approximate roots of a polynomial*, Crelle **278**(1974), 301–306.

School of Mathematics and Statistics
University of Sydney
New South Wales 2006
Australia