MATHEMATICS OF COMPUTATION
Volume 69, Number 231, Pages 1183–1191
S 0025-5718(00)01247-3
Article electronically published on March 2, 2000

IRREDUCIBILITY TESTING OVER LOCAL FIELDS

P. G. WALSH

ABSTRACT. The purpose of this paper is to describe a method to determine whether a bivariate polynomial with rational coefficients is irreducible when regarded as an element in $\mathbf{Q}((x))[y]$, the ring of polynomials with coefficients from the field of Laurent series in x with rational coefficients. This is achieved by computing certain associated Puiseux expansions, and as a result, a polynomial-time complexity bound for the number of bit operations required to perform this irreducibility test is computed.

1. INTRODUCTION

Factoring polynomials and testing polynomials for irreducibility is a fundamental problem in algorithmic mathematics. In [15], it was proved that factoring univariate polynomials with rational coefficients has polynomial-time complexity. This work was generalized to multivariate polynomials in [14], and to univariate polynomials with algebraic coefficients in [12] and [13]. In [4], Chistov proved the existence of polynomial-time complexity bounds for factoring polynomials with coefficients from local fields, such as $\mathbf{Q}_p$, the field of p-adic rationals, and $\mathbf{F}_p((x))$, the field of formal Laurent series with coefficients from the finite field with p elements. For more on the recent history of this subject the reader is referred to the excellent survey papers [8] and [9].

The purpose of this paper is to describe a method to determine if a polynomial F in $\mathbf{Q}[x, y]$ is irreducible when regarded as a polynomial in $\mathbf{Q}((x))[y]$, where $\mathbf{Q}((x))$ denotes the field of formal Laurent series in the variable x with rational coefficients and the usual rules of multiplication and addition. The method described here is based on the computation of the singular part of the Puiseux expansions at $x = 0$ of the algebraic function y defined by the equation $F(x, y) = 0$. By applying the recent result proved in [21], we show that the method described in this paper has a polynomial-time complexity bound for the number of bit operations. We will also prove the existence of a similar complexity bound for determining the irreducibility of F in the ring $\overline{\mathbf{Q}}((x))[y]$, where $\overline{\mathbf{Q}}$ denotes an algebraic closure of $\mathbf{Q}$. It will be the subject of future work to extend the results obtained here by developing a method to factor polynomials in $\mathbf{Q}((x))[y]$ and $\overline{\mathbf{Q}}((x))[y]$.

It is worth noting that by applying the results here to a transformation of $F(x, y)$ of the form $x' = x + a$, $a \in \mathbf{Q}$, one could prove a similar result with $\mathbf{Q}((x))$ replaced by $\mathbf{Q}((x - a))$.

Received by the editor September 5, 1994 and, in revised form, June 12, 1995.
1991 *Mathematics Subject Classification.* Primary 12Y05, 12E05.
Key words and phrases. Algebraic function, Puiseux expansion, irreducibility testing, computational complexity, local field.
This work constitutes part of the author's doctoral dissertation at the University of Waterloo.

In what follows we let $F \in \mathbf{Q}[x,y]$ be of degree m in x and n in y. Let $\mathrm{denom}(F)$ denote the least positive integer such that $\mathrm{denom}(F) \cdot F$ has integer coefficients, then the *height* of F, denoted by $\mathrm{ht}(F)$ is the maximum of the absolute values of the coefficients of $\mathrm{denom}(F) \cdot F$. Let $\mathrm{disc}_y(F)$ denote the discriminant of F, where F is regarded as a polynomial in y. For our main result we will assume that this discriminant is nonzero, which of course means that the roots of F in any algebraic closure of $\mathbf{Q}(x)$ are distinct, and equivalent to the condition that the greatest common divisor of F and the derivative of F with respect to y is 1.

By a *bit* operation we will always mean the addition or multiplication of two bits. The complexity of algorithms in this paper will be measured in bit operations, and we appeal to [10, Theorem A, p. 260], which states that for any $\varepsilon > 0$ the multiplication of two k-bit integers requires $O(k^{1+\varepsilon})$ bit operations. In [21] it was shown that the singular part of an algebraic function can be computed in

$$T(m,n,h,\varepsilon) := O(n^{32+\varepsilon} m^{4+\varepsilon} \log^{2+\varepsilon}(h)) \tag{1}$$

bit operations. We discuss this in more detail in Theorem A (in Section 4), but state our results in terms of this quantity.

Theorem 1. *Let F be as above. Given $\varepsilon > 0$, determining whether F is irreducible in $\mathbf{Q}((x))[y]$ can be accomplished in*

$$O(n \cdot T(nm, n, h, \varepsilon))$$

bit operations.

The reader may be somewhat alarmed by the large exponent of n in this result. This is a direct result of the large exponents which appear in the complexity bounds in [15] and [13]. Any improvement on the complexity of reducing lattice bases will yield an improvement to Theorem 1.

Abhyankar [1] has given an interesting criterion for a polynomial $F \in \mathbf{K}[x,y]$ to be irreducible in $\mathbf{K}((x))[y]$, where $\mathbf{K}$ is algebraically closed and of characteristic zero. Theorem 1 can be thought of as a rational version of Abhyankar's result, although it would be interesting to remove the restriction of algebraic closedness from Abhyankar's method and thereby obtain a true rational version of his result.

Theorem 1 has application to diophantine analysis. In [19] the author computed upper bounds to integer solutions of diophantine equations of the form $F(x,y) = 0$, where F is assumed to be irreducible in $\mathbf{Q}[x,y]$ but reducible as a polynomial in $\mathbf{Q}((x^{-1}))[y]$. Polynomials which satisfy this condition are referred to as satisfying Runge's Condition. From Theorem 1 and the main result of [14], one can easily deduce the following.

Corollary 1. *There is a polynomial-time algorithm to decide if a polynomial satisfies Runge's Condition.*

2. Notation

A considerable amount of notation will be required in this paper. Some of it is given below, while more will be introduced in succeeding sections.

By $\mathbf{Q}, \mathbf{Z}, \overline{\mathbf{Q}}$, and $\mathbf{C}$ we mean the field of rational numbers, the rational integers, an algebraic closure of $\mathbf{Q}$, and the field of complex numbers, respectively.

Let α denote an algebraic number defined by the polynomial

$$P(x) = a_d x^d + \cdots + a_0, \quad a_d \neq 0,$$

where each $a_i \in \mathbf{Z}$, and $\gcd(a_1, \ldots, a_d) = 1$, that is $P(\alpha) = 0$, and no polynomial of degree less than d has α as a root. Then $P_\alpha(x) = P(x)$ will be used to denote the *defining polynomial* for $\alpha, \deg P = \deg(\alpha) = d$ is the *degree* of $\alpha, \mathrm{lc}(\alpha) = a_d$ is the *leading coefficient* of $P_\alpha(x)$, and we define $\overline{\alpha}$ to be the algebraic integer $\mathrm{lc}(\alpha) \cdot \alpha$. Also, we define $\mathrm{ht}(\alpha)$ to be the *height* of α, which is the maximum of the absolute values of the coefficients of $P_\alpha(x)$.

Assume that $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(d)}$ are the (necessarily distinct) roots of $P_\alpha(x)$. Then they are referred to as the *algebraic conjugates* of α, and there are d embeddings $\sigma_1, \sigma_2, \ldots, \sigma_d$ of the field extension $\mathbf{Q}(\alpha)$ generated by α into $\overline{\mathbf{Q}}$ such that $\sigma_i(\alpha) = \alpha^{(i)}$ for $1 \leq i \leq d$.

Finally, given a field extension K of finite degree over $\mathbf{Q}$, and $\alpha \in K$ such that $K \in \mathbf{Q}(\alpha)$, then α is said to be *primitive.*

3. Preliminary results on Puiseux expansions

Let $F(x,y) \in \mathbf{Q}[x,y]$, and write F as

$$F(x,y) = A_n(x)y^n + A_{n-1}(x)y^{n-1} + \cdots + A_0(x), \; A_n \neq 0. \tag{2}$$

For a positive integer e let $x^{1/e}$ denote a formal eth root of x. If $\mathrm{disc}_y(F)$ is nonzero, that is, squarefree when regarded as a polynomial in y in $\mathbf{Q}[x,y]$, then Puiseux's theorem (for example see [2], [16], or [18]) asserts the existence of n distinct series

$$y_i(x) = \sum_{k=f_i}^{\infty} a_{k,i}(x^{1/e_i})^k \quad (1 \leq i \leq n), \tag{3}$$

with $e_i, f_i \in \mathbf{Z}$, $e_i > 0$, and $a_{k,i} \in \overline{\mathbf{Q}}$ such that

$$F(x,y) = A_n(x) \prod_{i=1}^{n} (y - y_i(x)). \tag{4}$$

For $i = 1, \ldots, n$, $y_i(x)$ is called a *Puiseux expansion* at $x = 0$ of the algebraic function y defined by $F(x,y) = 0$, and the positive integer e_i is the *ramification index* of the expansion $y_i(x)$. For each $i = 1, \ldots, n$, the ramification index e_i is defined to be minimal, in the sense that for any divisor d of e_i there is an index k with $a_{k,i} \neq 0$ such that d does not divide k.

In what follows we let

$$y(x) = \sum_{k=f}^{\infty} a_k(x^{1/e})^k \tag{5}$$

denote one of the n expansions described above.

Let ζ_e denote the primitive eth root of unity. The *branch* of Puiseux expansions containing $y(x)$ is the set

$$B(y(x)) = \left\{ \sum_{k=f}^{\infty} a_k(\zeta_e^i x^{1/e})^k; \quad 0 \leq i \leq e-1 \right\}. \tag{6}$$

Note that the set of all n expansions in (3) is partitioned into branches, with each expansion in a particular branch having the same ramification index, and the number of expansions in a particular branch being equal to the ramification index of each expansion in that branch.

Let $\mathbf{K} = \mathbf{Q}(a_f, a_{f+1}, \dots)$, then it is evident that $[\mathbf{K} : \mathbf{Q}] < \infty$. Let $s = [\mathbf{K} : \mathbf{Q}]$, and let $\sigma_1, \sigma_2, \dots, \sigma_s$ denote the embeddings of $\mathbf{K}$ into $\overline{\mathbf{Q}}$. The *conjugacy class* of expansions containing $y(x)$ is the set

$$(7)\qquad C(y(x)) = \left\{ \sum_{k=f}^{\infty} \sigma_j(a_k)(\zeta_e^i x^{1/e})^k; \quad 1 \le j \le s, 0 \le i \le e-1 \right\}.$$

The set of all n expansions in (3) is partitioned into conjugacy classes, and in fact one can easily see that $C(y(x))$ is the set of all expansions appearing in one of the branches $B(y_\sigma(x))$, where $y_\sigma(x) = \sum_{k=f}^{\infty} \sigma(a_k) x^{k/e}$. Furthermore, it is straightforward to check that distinct branches are disjoint, and that each branch of the form $B(y_\sigma(x))$ contains precisely e expansions. Therefore the conjugacy class of $y(x), C(y(x))$, contains es_1 elements for some positive integer s_1.

The following result shows that our main task is to compute the order of $C(y(x))$.

Lemma 1. *Assume that* $\operatorname{disc}_y(F) \ne 0$, *and let* $y_1(x), y_2(x), \dots, y_{es_1}(x)$ *denote the* es_1 *distinct Puiseux expansions in* $C(y(x))$. *Then* $\prod_{i=1}^{es_1}(y - y_i(x))$ *is irreducible in* $\mathbf{Q}((x))[y]$. *Also, if* $y_1(x), \dots, y_e(x)$ *denote the Puiseux expansions in* $B(y(x))$, *then* $\prod_{i=1}^{e}(y - y_i(x))$ *is irreducible in* $\overline{\mathbf{Q}}((x))[y]$.

Proof. The product over $C(y(x))$ is the norm from $\overline{\mathbf{Q}}((x^{1/e}))$ to $\mathbf{Q}((x))$, extended to polynomials, of $(y - y_i(x))$. Since $(y - y_i(x))$ is evidently irreducible in $\overline{\mathbf{Q}}((x^{1/e}))[y]$, it follows from [17, Theorem 2.1] that this product is a power of an irreducible factor in $\mathbf{Q}((x))[y]$. Since $\operatorname{disc}_y(F) \ne 0$, the n Puiseux expansions of the algebraic function y are distinct. Therefore the product over $C(y(x))$ must be irreducible. The second part of the lemma follows by the same argument with $\mathbf{Q}((x))$ replaced by $\overline{\mathbf{Q}}((x))$.

By Lemma 1 we see that the irreducible factor of $F(x, y)$ in $\mathbf{Q}((x))[y]$ with $(y - y(x))$ as a factor has degree es_1, where s_1 is the number of distinct branches of expansions in the conjugacy class $C(y(x))$. Our goal now is to describe the number s_1.

Definition. Let σ be an embedding of $\mathbf{K}$ into $\overline{\mathbf{Q}}$. We say that σ is *redundant relative to* $y(x)$ (or simply *redundant*) if the expansion $y_\sigma(x) = \sum_{k=f}^{\infty} \sigma(a_k) x^{k/e}$ is in the branch $B(y(x))$. Equivalently, σ is redundant if there is a positive integer t such that $\sigma(a_k) = a_k \zeta_e^{tk}$ for all $k \ge f$.

Lemma 2. *Let* s_0 *denote the number of redundant embeddings relative to* $y(x)$, *let* e *denote the ramification index of* $y(x)$, *and let* $s = [\mathbf{K} : \mathbf{Q}]$. *Then* $C(y(x))$ *contains precisely* es/s_0 *distinct elements.*

Proof. We let $\mathbf{1_K}$ denote the identity map on $\mathbf{K}$. Let σ and γ denote embeddings of $\mathbf{K}$ into $\overline{\mathbf{Q}}$. We will write $\sigma \sim \gamma$ if the branch containing the expansion $\sum_{k=1}^{\infty} \sigma(a_k) x^{\gamma_k}$ also contains $\sum_{k=1}^{\infty} \gamma(a_k) x^{\gamma_k}$. It is easy to check that this is an equivalence relation on the set of embeddings. We will prove Lemma 2 by showing that each equivalence class of embeddings $E(\sigma) = \{\gamma; \gamma \sim \sigma\}$ contains precisely s_0 elements. To show this we prove that for each $\sigma : \mathbf{K} \to \overline{\mathbf{Q}}$,

$$(8)\qquad E(\sigma) = \{\sigma_1 \vartheta; \vartheta \in E(\mathbf{1_K})\},$$

where σ_1 is some fixed extension of σ to $\mathbf{K}(\zeta_e)$, where ζ_e is some primitive eth root of unity.

Let $\sigma : \mathbf{K} \to \overline{\mathbf{Q}}$, and let σ_1 be some fixed extension of σ to $K(\zeta_e)$ defined by $\sigma_1(\zeta_e) = \zeta_e^j$. Note that ζ_e^j must also be a primitive eth root of unity, and hence $\gcd(e, j) = 1$.

Let $\vartheta \in E(\mathbf{1_K})$ and let i be the integer with $0 \le i \le e-1$ such that $\vartheta(a_k) = a_k\zeta_e^{ik}$ for all $k \ge f$. Then

$$\sigma_1\vartheta(a_k) = \sigma_1(a_k\zeta_e^{ik}) = \sigma(a_k)\zeta_e^{ijk}$$

for all $k \ge f$, and so $\sigma_1\vartheta \in E(\sigma)$. Now let σ_1^{-1} denote the inverse of σ_1,

$$\sigma_1^{-1} : \sigma_1(\mathbf{K}) \to \mathbf{K},$$

and let j^{-1} denote the inverse of $j (\bmod e)$. Then $\sigma_1(\zeta_e) = \zeta_e^{j^{-1}}$. For $\gamma \in E(\sigma)$ put $\vartheta = \sigma_1^{-1}\gamma$. Because $\gamma \in E(\sigma)$, there is an integer j_1 such that $\gamma(a_k) = \sigma(a_k)\zeta_e^{j_1k}$ for all $k \ge f$. Therefore, $\vartheta(a_k) = \sigma_1^{-1}\gamma(a_k) = \sigma_1^{-1}(\sigma(a_k)\zeta_e^{j_1k}) = a_k\alpha_e^{j^{-1}j_1k}$ for all $k \ge f$, and hence $\gamma = \sigma_1\vartheta$. Thus, we have that (8) holds.

To see that all $\sigma_1\vartheta$ are distinct, assume on the contrary that $\sigma_1\vartheta_1(a_k) = \sigma_1\vartheta_2(a_k)$ for all $k \ge f$, where $\vartheta_1(a_k) = a_k\alpha_e^{j_1k}$ for all $k \ge f$ and $\vartheta_2(a_k) = a_k\alpha_e^{j_2k}$ for all $k \ge f$. It follows that $\zeta_e^{jj_1k} = \zeta_e^{jj_2k}$ for all k with $a_k \ne 0$. Therefore $jj_1k \equiv jj_2k (\bmod e)$ for all k with $a_k \ne 0$. By the minimality condition of the ramification index e, it follows that $jj_1 \equiv jj_2 (\bmod e)$. But $\gcd(e, j) = 1$, hence $j_1 \equiv j_2 (\bmod e)$, and hence $\vartheta_1 = \vartheta_2$. This completes the proof of Lemma 2.

4. The singular part of $y(x)$

We will henceforth write $y(x)$ in the form

$$y(x) = \sum_{k=1}^{\infty} a_k x^{\gamma_k}, \tag{9}$$

where $a_k \ne 0$ for all $k \ge 1$, $\gamma_k = f_k/e_k$ with $\gcd(f_k, e_k) = 1$ for those k with $f_k \ne 0$, and $\gamma_{k+1} > \gamma_k$ and $e_k > 0$ for all $k \ge 1$. We will assume throughout this section that $f_1 \ge 0$, for it will be seen later that this will cause no restriction.

Definition. The *singular part* of $y(x)$ is the minimal initial partial sum

$$y_T(x) = \sum_{k=1}^{T} a_k x^{\gamma_k} \quad (a_k \ne 0), \tag{10}$$

such that the sum of the first T terms of any other Puiseux expansion of y does not equal $y_T(x)$.

The following result is critical to our algorithm. It shows that the singular part of $y(x)$ contains much of the necessary information about $y(x)$.

Lemma 3. *Let all of the notation be as above. Then*

1. $\mathbf{K} = \mathbf{Q}(a_1, a_2, \ldots, a_T)$ *and hence* $s = [\mathbf{Q}(a_1, \ldots, a_T) : \mathbf{Q}]$.
2. $e = \operatorname{lcm}(e_1, e_2, \ldots, e_T)$.
3. $T \le 4mn^2$.

Proof. 1. This is an immediate consequence of [11, Theorems 6.1 and 5.5], and also follows from [7, Theorem 4.5].
2. This is in [11, Theorem 6.1], and was rediscovered in [6].
3. This follows easily from [11, Corollary 6.1].

In [21], the author proved the following result which is the basis for the results proved here.

Theorem A. *Let F be as in (2), and assume that* $\operatorname{disc}(F)$ *is nonzero, and that $A_n(0) \neq 0$. Let m, n, and h denote the degree of F in x, the degree of F in y, and the height of F, respectively. Then for any $\varepsilon > 0$ the singular part of one Puiseux expansion at $x = 0$ of the algebraic function y defined by $F(x, y) = 0$ can be computed in $O(n^{32+\varepsilon} m^{4+\varepsilon} \log^{2+\varepsilon}(h))$ bit operations.*

Let $T(m, n, h, \varepsilon)$ be as in (1). By part 2 of Lemma 3 and Theorem A, we have the following.

Theorem 2. *Let $F \in \mathbf{Q}[x, y]$ be of degree m in x, n in y, of height h. Then for $\varepsilon > 0$, deciding if F is irreducible in $\overline{\mathbf{Q}}((x))[y]$ can be accomplished in $O(T(nm, n, h, \varepsilon))$ bit operations.*

Proof. We may assume that $\operatorname{disc}_y F \neq 0$; otherwise F would have multiple roots for y, and hence would be reducible in $\overline{\mathbf{Q}}((x))[y]$. This condition can easily be checked within the number of bit operations given in the statement of the theorem. Let F be as in (2), then replacing $F(x, y)$ by $\widetilde{F}(x, y) = x^{\mu} F(x, yx^{-\lambda})$, for suitably chosen nonnegative integers μ and λ (for example $\mu = mn - \operatorname{ord}_x A_n$ and $\lambda = m$ will do) we can assume that the leading coefficient of F does not vanish at $x = 0$, and hence that all of the Puiseux expansions of the algebraic function y defined by $F(x, y) = 0$ have no terms with negative exponents. Moreover, by this choice of μ and λ, the resulting polynomial will have degree in x no greater than $(n+1)m$. Thus, in order to determine if F is irreducible in $\overline{\mathbf{Q}}((x))[y]$, it suffices to compute the singular part of one Puiseux expansion and compare the ramification index of that expansion to the degree in y of F. The result now follows from Theorem A.

By Lemma 3, in order to compute the quantities s and e of Lemma 2, it suffices to compute the singular part of the Puiseux expansion $y(x)$. It remains to describe a method to compute the quantity s_0, the number of redundant embeddings relative to $y(x)$.

5. The computation of s_0

In this section we will describe a method to compute the value s_0. We will require notation from [21], wherein an algorithm to compute the singular part of $y(x)$ is described.

Let $\mathbf{K} = \mathbf{Q}(a_1, a_2, \dots)$, which by Lemma 3 is equal to $\mathbf{Q}(a_1, a_2, \dots, a_T)$. As before, let $s = [\mathbf{K} : \mathbf{Q}]$, and $\sigma_1, \dots, \sigma_s$ the embeddings of $\mathbf{K}$ into $\overline{\mathbf{Q}}$. Let S denote the set of redundant embeddings of $\mathbf{K}$ into $\overline{\mathbf{Q}}$ relative to $y(x)$, so that $s_0 = |S|$. For $1 \leq i \leq T$, define $\overline{a_i} = \operatorname{lc}(P_{a_i}) \cdot a_i$, and let $t_1, t_2, \dots, t_T$ be integers in the range $0 \leq t_i \leq n^2$ with the property that

$$\alpha_i = \overline{a_1} + t_2 \overline{a_2} + \cdots + t_i \overline{a_i}$$

denotes the primitive algebraic integer, with minimal polynomial $P_{\alpha_i}(x)$, computed in [21, Algorithm 3.1], with the property that $\mathbf{Q}(a_1, \dots, a_i) = \mathbf{Q}(\alpha_i)$. Also, for $1 \leq i \leq T$, let $P_{i,i}(x)$ denote the polynomial of degree at most $\deg(P_{\alpha_i}) - 1$, with rational coefficients, computed in [21, Algorithm 3.1] which satisfies $a_i = P_{i,i}(\alpha_i)$.

For $1 \leq i \leq T$ and $0 \leq t \leq e - 1$ define

$$\alpha_{i,t} = \overline{a_1} \zeta_{e_1}^{tf_1} + t_2 \overline{a_2} \zeta_{e_2}^{tf_2} + \cdots + t_i \overline{a_i} \zeta_{e_i}^{tf_i},$$

where, in (9), $\gamma_i = f_i/e_i$ is a reduced fraction and ζ_{e_j} is an e_jth root of unity for $1 \leq j \leq i$. For $1 \leq i \leq T$ and $0 \leq t \leq e-1$, $P_{\alpha_{i,t}}(x)$ will denote the minimal polynomial of $\alpha_{i,t}$.

Lemma 4. *The number s_0 is precisely the number of values of t with $0 \leq t \leq e-1$ such that $P_{\alpha_{i,t}}(x) = P_{\alpha_i}(x)$ and $a_i\zeta_{e_i}^{tf_i} = P_{i,i}(\alpha_{i,t})$ for all i in the range $1 \leq i \leq T$.*

Proof. Let σ be a redundant embedding, then there is an integer t such that $\sigma(a_i) = a_i\zeta_{e_i}^{tf_i}$ for all $i \geq 1$. From the way in which α_i is defined, it follows that $\sigma(\alpha_i) = \alpha_{i,t}$ for all i in the range $1 \leq i \leq T$, which is the same as $P_{\alpha_{i,t}}(x) = P_{\alpha_i}(x)$ for all $1 \leq i \leq T$. Also, from the definition of the polynomial $P_{i,i}(x)$,

$$a_i\zeta_{e_i}^{tf_i} = \sigma(a_i) = \sigma(P_{i,i}(\alpha_i)) = P_{i,i}(\sigma(\alpha_i)) = P_{i,i}(\alpha_{i,+})$$

for all i in the range $1 \leq i \leq T$.

It suffices now to show that if t is an integer for which the two conditions in the statement of Lemma 4 hold, then there is an embedding σ of K into $\overline{\mathbf{Q}}$ for which $\sigma(a_i) = a_i\zeta_{e_i}^{tf_i}$ for all $i \geq 1$. By the definition of T, it is sufficient to show that there is an embedding σ for which $\sigma(a_i) = a_i\zeta_{e_i}^{tf_i}$ for all $1 \leq i \leq T$. This is accomplished by induction on $i = 1, \ldots, T$.

Let $i = 1$. Then since $P_{\alpha_{1,t}}(x) = P_{\alpha_1}(x)$, there is an embedding σ of $\mathbf{Q}(a_1)$ into $\overline{\mathbf{Q}}$ for which $\sigma(\alpha_1) = \alpha_{1,t}$. Therefore,

$$a_1\zeta_{e_1}^{tf_1} = P_{1,1}(\alpha_{1,1}) = P_{1,1}(\sigma(\alpha_1)) = \sigma(P_{1,1}(\alpha_1)) = \sigma(a_1),$$

from which it follows that $\sigma(\overline{a_1}) = \overline{a_1}\zeta_{e_1}^{tf_1}$.

Let k be integer in the range $1 \leq k \leq T-1$. Assume that σ is an embedding of $\mathbf{Q}(a_1, \ldots, a_k)$ into $\overline{\mathbf{Q}}$, with the property that $\sigma(a_i) = a_i\zeta_{e_i}^{tf_i}$ for all $1 \leq i \leq k$. Since we know that $P_{\alpha_{k+1,t}}(x) = P_{\alpha_{k+1}}(x)$, there is another embedding σ_1 of $\mathbf{Q}(a_1, \ldots, a_{k+1})$ into $\overline{\mathbf{Q}}$ such that $\sigma_1(\alpha_{k+1}) = \alpha_{k+1,t}$. Therefore,

$$a_{k+1}\zeta_{e_{k+1}}^{tf_{k+1}} = P_{k+1,k+1}(\alpha_{k+1,t}) = P_{k+1,k+1}(\sigma_1(\alpha_{k+1})) = \sigma_1(a_{k+1}),$$

from which it follows that $\overline{a_{k+1}}\zeta_{e_{k+1}}^{tf_{k+1}} = \sigma_1(\overline{a_{k+1}})$. Thus,

$$\begin{aligned}\alpha_{k+1,t} &= \overline{a_1}\zeta_{e_1}^{tf_1} + \cdots + t_{k+1}\overline{a_{k+1}}\zeta_{e_{k+1}}^{tf_{k+1}} \\ &= \sigma(\overline{a_1} + \cdots + t_k\overline{a_k}) + \sigma_1(t_{k+1}\overline{a_{k+1}})\end{aligned}$$

and

$$\begin{aligned}\alpha_{k+1,t} = \sigma_1(\alpha_{k+1}) &= \sigma_1(\overline{a_1} + \cdots + t_{k+1}\overline{a_{k+1}}) \\ &= \sigma_1(\alpha_k) + \sigma_1(t_{k+1}\overline{a_{k+1}}).\end{aligned}$$

Therefore, $\sigma(\alpha_k) = \sigma_1(\alpha_k)$ and it follows that $\sigma_1(a_{k+1}) = a_{k+1}\zeta_{e_{k+1}}^{tf_{k+1}}$. But since σ and σ_1 agree on $\mathbf{Q}(\alpha_k) = \mathbf{Q}(a_1, \ldots, a_k)$, it follows that $\sigma_1(a_i) = a_i\zeta_{e_i}^{tf_i}$ for all $1 \leq i \leq k+1$.

6. Proof of Theorem 1

As in the proof of Theorem 2 we may assume that $\operatorname{disc}_y F \neq 0$. Also, by a transformation of F described in the proof of Theorem 2 we may assume that the Puiseux expansions of the algebraic function y at $x = 0$ have no terms with negative exponents. In this case F is being replaced by another polynomial, say $\widetilde{F}$, whose height and degree in y is the same, but whose degree in x is bounded by $(n+1)m$. Moreover, it is a simple exercise to see that F is irreducible if and only if $\widetilde{F}$ is also.

In order to decide if $\widetilde{F}$ is irreducible in $\mathbf{Q}((x))[y]$ we need to compute the numbers e, s, and s_0 which are associated to one of the Puiseux expansions, say $y(x)$, of y, the algebraic function defined by $\widetilde{F}(x,y) = 0$, and check whether or not $n = es/s_0$. By Lemma 3, the values e and s are computed once the singular part of $y(x)$ is computed, and so the only difficulty now remains in the computation of s_0. This is accomplished by determining which values of t, with $0 \leq t \leq e-1$, have the property that there is an embedding σ of $\mathbf{Q}(a_1, \ldots, a_T)$ into $\overline{\mathbf{Q}}$ of the form $\sigma(a_i) = a_i\zeta_{e_i}^{tf_i}$ for all $i = 1, \ldots, T$. By Lemma 4, this can be accomplished by deciding which values of t, with $0 \leq t \leq e-1$, have the property that $P_{\alpha_{i,t}}(x) = P_{\alpha_i}(x)$ and $a_i\zeta_{e_i}^{tf_i} = P_{i,i}(\alpha_{i,t})$ for all $i = 1, \ldots, T$. For each fixed i, with $1 \leq i \leq T$, this reduces to simply computing the polynomial $P_{\alpha_{i,t}}(x)$, in the course of computing the singular part of the Puiseux expansion $y_i(x) = \sum_{i=1}^{\infty} a_i\zeta_{e_i}^{tf_i}x^{f_i/e_i}$, in the same manner that the polynomial $P_{\alpha_i}(x)$ is computed during the computation of the singular part of $y(x)$, and computing the representation of $a_i\zeta_{e_i}^{tf_i}$ in the field $\mathbf{Q}(\alpha_{i,t})$ in the same way that the representation of a_i in $\mathbf{Q}(\alpha_i)$ is obtained during the computation of the singular part of $y(x)$. In other words, it suffices to compute all e Puiseux expansions in the branch $B(y(x))$. Thus the total work is no more than e times the work to compute the singular part of the expansion $y(x)$. Theorem 1 now follows from Theorem A, the bounds for the degrees and height of $\widetilde{F}$ given above, and the fact that $e \leq n$.

Acknowledgments

The author would like to thank Cam Stewart for his many helpful suggestions, and Hendrik Lenstra for pointing out an error in an earlier version of this work.

References

1. S. S. Abhyankar, *Irreducibility criterion for germs of analytic functions of two complex variables*, Adv. Math. **74** (1989), 190–257. MR **90h**:32018
2. G. A. Bliss, *Algebraic functions*, Amer. Math. Soc. Colloq. Publ. **16** (1933).
3. A. L. Chistov, *Polynomial complexity of the Newton-Puiseux algorithm*, Lecture Notes in Computer Science **233** (1986), 247–255. CMP 19:07
4. ———, *Efficient factoring polynomials over local fields and its applications*, Proc. ICM 1990, (1991), 1509–1519. MR **93e**:11152
5. J. Coates, *Construction of rational functions on a curve*, Proc. Cambridge Philos. Soc. **68** (1970), 105–123. MR **41**:3477
6. D. L. Hilliker, *An algorithm for computing the values of the ramification index in the Puiseux series expansions of an algebraic function*, Pacific J. Math. **118**, no. 2 (1985), 427–435. MR **86i**:11068
7. D. L. Hilliker and E. G. Straus, *Determination of bounds for the solutions to those binary diophantine equations that satisfy the hypotheses of Runge's theorem*, Trans. Amer. Math. Soc. **280** (1983), 637–657. MR **85c**:11031
8. E. Kaltofen, "Polynomial Factorization 1982–1986", in *Computers and Mathematics*, Lecture Notes in Pure and Applied Mathematics **125** (1990), 285–309. MR **92f**:12001
9. ———, "Polynomial Factorization 1987–1991", In *Proceedings of Latin* '92, Lecture Notes in Computer Science **583** (1992), 294–313.
10. D. Knuth, *The Art of Computer Programming*, Vol. 2: *Seminumerical Algorithms*, Addison-Wesley, Reading, MA, 1969. MR **44**:3531
11. H. T. Kung and J. F. Traub, *All algebraic functions can be computed fast*, J. Assoc. Comput. Mach. **25** (1978), 246–260. MR **80a**:68042
12. S. Landau, *Factoring polynomials over algebraic number fields*, Siam J. Comput. **14**, no. 1 (1985), 184–195. MR **86d**:11102
13. A. K. Lenstra, *Factoring polynomials over algebraic number fields*, Proc. EuroCal. 1983, Lecture Notes in Computer Science **162** (1983), 245–254. MR **86g**:12001b

14. ———, *Factoring multivariate integral polynomials*, Theoret. Comp. Sci. **34** (1984), 207–213. MR **86g:**12001a

→ A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534. MR **84a:**12002

16. V. Puiseux, *Recherches sur les fonctions algébriques*, J. Math. Pures Appl. **15** (1850), 365–480.

17. B. M. Trager, *Algebraic factoring and rational function integration*, Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation, 219–226.

18. R. J. Walker, *Algebraic Curves*, Princeton University Press, Princeton, New Jersey, 1950. MR **11:**387e

19. P. G. Walsh, *A quantitative version of Runge's theorem on diophantine equations*, Acta Arith. **62** (1992), 157–172. MR **94a:**11037

20. ———, *The Computation of Puiseux Expansions and Runge's Theorem on Diophantine Equations*, Ph.D. Thesis, University of Waterloo, Waterloo, Ontario, Canada, 1994.

21. ———, *A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function*, Math. Comp., Posted on February 16, 2000, PII S 0025-5718(00)01246-1

Department of Mathematics, University of Ottawa, Ontario, Canada
E-mail address: `gwalsh@mathstat.uottawa.ca`