MATHEMATICS OF COMPUTATION
Volume 69, Number 231, Pages 1167–1182
S 0025-5718(00)01246-1
Article electronically published on February 16, 2000

A POLYNOMIAL-TIME COMPLEXITY BOUND FOR THE COMPUTATION OF THE SINGULAR PART OF A PUISEUX EXPANSION OF AN ALGEBRAIC FUNCTION

P. G. WALSH

Dedicated to Wolfgang Schmidt on the occasion of his sixtieth birthday.

Abstract. In this paper we present a refined version of the Newton polygon process to compute the Puiseux expansions of an algebraic function defined over the rational function field. We determine an upper bound for the bit-complexity of computing the singular part of a Puiseux expansion by this algorithm, and use a recent quantitative version of Eisenstein's theorem on power series expansions of algebraic functions to show that this computational complexity is polynomial in the degrees and the logarithm of the height of the polynomial defining the algebraic function.

1. Introduction

In [11] a method for computing the Puiseux expansions of an algebraic function is described. The method is a combination of two procedures. The first procedure goes back to Puiseux [17] and is described in [22] and [1]. This procedure is used in [11] to compute the singular part of a Puiseux expansion. Once the singular part is computed by this method, one then uses a second procedure to compute as many terms of the expansion as desired, in a very simple and efficient manner. The purpose of this paper is to provide a refined, ready-to-implement, version of the procedure to compute the singular part of a Puiseux expansion at $x = 0$ of an algebraic function y defined by $F(x, y) = 0$, with $F \in \mathbf{Q}[x, y]$, and apply a recent quantitative version of Eisenstein's theorem on power series expansions of algebraic functions in [8] to prove that the complexity of this algorithm is polynomial in $\deg_x F$, $\deg_y F$, and the logarithm of the height of F.

In [11], a polynomial complexity bound for the number of coefficient operations is computed. Unfortunately, this analysis does not take into consideration the size of the coefficients appearing in F, and hence does not provide a polynomial complexity bound for the number of bit operations. It is worth noting that Chistov [3] has shown that the algorithm of Puiseux has polynomial-time bit-complexity, but no explicit complexity bound is determined. For other work on the computation of Puiseux expansions the reader is referred to [4], [5], and [7]. Note that in each

Received by the editor May 28, 1994 and, in revised form, March 21, 1995 and June 5, 1996.
1991 *Mathematics Subject Classification.* Primary 14H05, 11Y15.
Key words and phrases. Algebraic function, Puiseux expansion, Newton polygon, complexity.
This work constitutes part of the author's doctoral dissertation from the University of Waterloo.

of these papers, as in [11], a complexity bound for computing Puiseux expansions is computed which does not take into account the size of the integers involved in the calculations. We note that in this paper we only consider the case that the polynomial $F(x, y)$ defining the algebraic function has rational coefficients. One can generalize our result to the case that $F(x, y)$ has algebraic coefficients by employing the quantitative version of Eisenstein's theorem proved by Schmidt in [18].

There are several applications of a polynomial-time algorithm to compute the singular part of Puiseux expansions of an algebraic function. These include a polynomial-time algorithm to factor polynomials $F \in \mathbf{Q}[x, y]$ into irreducibles in $\mathbf{Q}((x))[y]$, a polynomial-time algorithm to compute an integral basis of an algebraic function field, a polynomial-time algorithm to resolve the singularities of an algebraic curve, and a polynomial-time algorithm to compute the genus of an algebraic curve. We remark that Theorem 1 solves an open problem stated in [18, p. 90], wherein several other applications of the result of Theorem 1 are discussed. Some of these applications will be the subject of future work, although a polynomial time algorithm to test the irreducibility in $\mathbf{Q}((x))[y]$ of a polynomial $F \in \mathbf{Q}[x, y]$ has been described in [23, Chapter 4].

Acknowledgments. The author would like to acknowledge Professor C. L. Stewart, Professor H. W. Lenstra, Jr., Professor A. Lenstra, and the referee for their helpful suggestions during the course of this work.

2. Notation and preliminary results

We now present some notation which will be used in this paper.

Let

$$F(x, y) = A_n(x)y^n + A_{n-1}(x)y^{n-1} + \cdots + A_0(x) \tag{2.1}$$

be a bivariate polynomial with rational coefficients such that $A_n(x) \neq 0$. The *denominator* of F, denoted by $\operatorname{denom}(F)$, is the smallest positive integer v such that vF has integer coefficients. The *height* of F, denoted by $\operatorname{ht}(F)$ is the maximum of $\operatorname{denom}(F)$ and the absolute value of the coefficients of $\operatorname{denom}(F) \cdot F$. Let

$$F(x) = \sum_{i=0}^{n} a_i x^i$$

be a univariate polynomial of degree n with complex coefficients. The *length* of F, denoted by $|F|$, is given by

$$|F| = \left(\sum_{i=0}^{n} |a_i|^2 \right)^{1/2}.$$

The leading coefficient of F is a_n, and is denoted by $\operatorname{lc}(F)$. If F is a nonzero polynomial with integer coefficients, then the *content* of F, denoted by $\operatorname{con}(F)$, is the greatest common divisor of its nonzero coefficients.

Let α represent an algebraic number. Then $P_\alpha(x)$ will denote the unique irreducible polynomial with integer coefficients, positive leading coefficient, and content equal to one, with α as a root. The denominator of α, denote $\operatorname{denom}(\alpha)$, is the smallest positive integer ν such that $\nu\alpha$ is an algebraic integer. If $\alpha = \alpha^{(1)}, \ldots, \alpha^{(r)}$ are the roots of $P_\alpha(x)$, then $\|\alpha\| = \max_{1 \leq i < r} |\alpha^{(i)}|$ is the *house* of α. If k is a subfield of $\mathbf{Q}(\alpha)$, then a defining polynomial of α over k will be denoted by $\widetilde{P}_\alpha$, where k will be made explicit so that no confusion will arise. Such a polynomial is only

required to be irreducible over the subfield k and have α as a root. Let $F(x)$ be a polynomial of degree m in $\mathbf{Q}(\alpha)[x]$, with $n = [\mathbf{Q}(\alpha)\colon \mathbf{Q}]$ and

$$F(x) = \sum_{i=0}^{m} \sum_{j=0}^{n-1} a_{i,j} \alpha^j x^i.$$

The $\mathbf{Q}(\alpha)$-*height* of F is given by

$$F_{\max} = \max_{i,j}\{|a_{i,j}|\}.$$

In every instance that this notation is used, α will be made explicit so that there is no ambiguity.

Let K be a field, and $F, G \in K[x,y]$, with $F(x,y) = A_n(x)y^n + \cdots + A_0(x)$ and $G(x,y) = B_m(x)y^m + \cdots + B_0(x)$, of degrees n and m in y, respectively. The *resultant* of F and G with respect to y, denoted by $\operatorname{res}_y(F,G)$, is the determinant of the $(n+m) \times (n+m)$ Sylvester matrix, whose entries are the coefficients of F and G regarded as polynomials in y. The reader is referred to [2, p. 24] for more details.

Let $F(x,y)$ be as in (2.1). Then the equation

$$F(x,y) = 0$$

defines an algebraic function y whose values depend on x. For any point z_0 in the extended complex plane $\mathbf{C} \cup \{\infty\}$, Puiseux's theorem asserts the existence of n distinct expansions of the form

$$y_i(x) = \sum_{k=f_i}^{\infty} c_{k,i} (z^{1/e_i})^k,$$

where $c_{f_i,i} \neq 0$, $z = x - z_0$ if $z_0 \in \mathbf{C}$, $z = x^{-1}$ if $z_0 = \infty$, and z^{1/e_i} is an e_ith root of z for $1 \le i \le n$. The integers e_i, $1 \le i \le n$, are the *ramification indices* of y at the point z_0. The ramification indices are positive integers bounded by n. We note that a ramification index e of a Puiseux expansion is defined to be minimal in the sense that for all prime divisors p of e there is an index k for which p does not divide k and $c_k \neq 0$.

Let

$$y(x) = \sum_{k=f}^{\infty} c_k z^{k/e} \tag{2.2}$$

be one of the Puiseux expansions of y at a point z_0. The *regularity index* of the expansion $y(x)$ is the least integer T^* with the property that no other Puiseux expansion of the algebraic function y at z_0 has the initial partial sum $\sum_{k=f}^{T^*} c_k z^{k/e}$. The *singular part* of the expansion $y(x)$ is defined as the initial sum

$$y_{T^*}(x) = \sum_{k=f}^{T^*} c_k z^{k/e}. \tag{2.3}$$

By the preliminary transformations described in [11, p. 247], it is sufficient to consider the case that $z_0 = 0$. The series $\sum_{k=0}^{\infty} c_{k+f} x^k$ is a root of the polynomial $H(x,y) = F(x^e, x^f y)$, and it is evident that $\deg_y H = n$, and $\deg_x H \le 2mn$. Therefore, it follows from [9, Theorem 4.5] that $T^* \le 4mn^2$.

Our object of study will be the computation of the singular part of the Puiseux expansion $y(x)$, which is of the form

$$y_T(x) = a_1 x^{\gamma_1} + \cdots + a_T x^{\gamma_1 + \cdots + \gamma_T}, \tag{2.4}$$

where T is the number of nonzero terms in the singular part of $y(x)$, $a_1, \ldots, a_T$ are nonzero algebraic numbers and $\gamma_1, \gamma_1 + \gamma_2, \ldots, \gamma_1 + \cdots + \gamma_T$ are nonnegative rational numbers given in reduced form. Note that $T \leq 4mn^2$, where $m = \deg_x F$ and $n = \deg_y F$.

What is meant by computing the expression in (2.4) is to have computed the reduced form of $\gamma_1 + \cdots + \gamma_i$ for $1 \leq i \leq T$, P_α where α is an algebraic integer with $\mathbf{Q}(\alpha) = \mathbf{Q}(a_1, \ldots, a_T)$, along with polynomials $P_i(x)$, $i = 1, \ldots, T$, with rational coefficients, of degree no greater than $[\mathbf{Q}(\alpha)\colon \mathbf{Q}] - 1$ such that $a_i = P_i(\alpha)$ for each i. This completely describes the element $y_T(x)$ of (2.4).

In the complexity analysis we will measure all steps in *bit operations*. By [10, p. 260, Theorem A], given any $\varepsilon > 0$, one arithmetic operation on two integers of size k-bits requires $O(k^{1+\varepsilon})$ bit operations.

Let $F(x, y)$ be as in (2.1), with $n = \deg_y F$, $m = \deg_x F$, and $h = \mathrm{ht}(F)$. The goal of this paper is to prove the following result.

Theorem 1. *Let $\varepsilon > 0$. The singular part $y_T(x)$ in (2.4) can be computed in $O(n^{32+\varepsilon} m^{4+\varepsilon} \cdot \log^{2+\varepsilon}(h))$ bit operations.*

By using the method of Kung and Traub in [11], after computing the singular part one can then compute as many terms of a Puiseux expansion as required in a very efficient manner. Using Theorem 1, one can compute a polynomial-time complexity bound for the number of bit operations required to compute k terms of a Puiseux expansion. We forgo this analysis.

We now state some known results which will be required for the complexity analysis given in the final section of this paper. The following quantitative version of Eisenstein's theorem follows immediately from the proof of [8, Theorem 1].

Theorem A. *Let $G \in \mathbf{Z}[x, y]$ be a nonzero polynomial which has no multiple factors when regarded as a polynomial in y. Let $m = \deg_x G$, $n = \deg_y G$, and $h = \mathrm{ht}(G)$. If the formal power series $y(x) = \sum_{k=0}^{\infty} b_k x^k$ satisfies $G(x, y(x)) = 0$, then there is an integer B with*

$$B < 4.8(8e^{-3} n^{4+2.74 \log n} e^{1.22n} h^2 (1+m)^2)^n, \tag{2.5}$$

for which $B^{m+k} b_k$ is an algebraic integer for all $k \geq 0$.

The important feature of this result is that B is singly exponential in the degrees of the polynomial $G(x, y)$. A singly exponential result was first obtained by Wolfgang Schmidt in [18]. Quantitative versions of Eisenstein's theorem prior to this, for example in [6] which had B of the form h^u with $u = (4n)^{3nm}$, would not have been sufficient to prove a polynomial-time bit-complexity bound for the computation of Puiseux expansions. The following result of [14] is A. Lenstra's extension to algebraic number fields of the well-known result of [15] on factoring polynomials with rational coefficients.

Theorem B. *Let D be a positive integer and let α be an algebraic integer of degree m. Let $f(x)$ be a monic polynomial in $\frac{1}{D}\mathbf{Z}[\alpha][x]$ of degree $n \geq 0$. Then there is an algorithm to factor $f(x)$ into monic irreducible polynomials in $\frac{1}{dD}\mathbf{Z}[\alpha][x]$, $d = \mathrm{disc}(P_\alpha)$, which requires $O(n^6 m^6 + n^5 m^6 \log(m \cdot |P_\alpha|) + n^5 m^5 \log(D \cdot f_{\max}))$*

arithmetic operations. The size of the integers on which these operations are performed is

$$O(n^3m^3 + n^2m^3 \log(m \cdot |P_\alpha|) + n^2m^2 \log(D \cdot f_{\max})).$$

Moreover, if $h(x)$ is an irreducible factor of $f(x)$, then

$$h_{\max} \leq f_{\max} \left[2(n+1)^2 m(m-1)^{m-1} \binom{2r}{r} \right]^{-1/2} |P_\alpha|^{2(m-1)} |\operatorname{disc}(P_\alpha)|^{-1/2},$$

where $r = \deg_x h$.

We will also require the following result on the complexity of computing the greatest common divisor of univariate polynomials. The rational case can be found in [2], while the number field case is in [13]. Recall that the greatest common divisor of two polynomials is assumed to be monic.

Theorem C.

i. *Let f and g be polynomials in $\mathbf{Q}[x]$, of degree m and n, respectively. Then $\gcd(f, g)$ can be computed in $O(\max\{\log|f|, \log|g|\}^2 \cdot \max\{m, n\}^4)$ bit operations.*

ii. *Let α be an algebraic integer of degree m. Let f and g be polynomials in $\mathbf{Z}[\alpha][x]$ of degree bounded by n. Then the greatest common divisor of f and g in $\mathbf{Q}[\alpha][x]$ can be computed in*

$$O((n^5m^3 + n^4m^5) \log^2(n \cdot \max\{f_{\max}, g_{\max}\} \cdot (\operatorname{ht}(P_\alpha))^m))$$

bit operations.

3. The Newton polygon algorithm

In this section we give a detailed description of the Newton polygon process. One iteration of this procedure computes one term of the Puiseux expansion $y(x)$, at $x = 0$, of the algebraic function y defined by $F(x, y) = 0$, where $F \in \mathbf{Q}[x, y]$, and is given in (2.1). We let $n = \deg_y F$, $m = \deg_x F$, $h = \operatorname{ht}(F)$, and we make the assumption that $\operatorname{disc}(F) \neq 0$, so that the n Puiseux expansions of F at $x = 0$ are distinct. By the transformation described in [11, p. 247], it is sufficient to consider the case that $A_n(0) \neq 0$. In this case, none of the Puiseux expansions of y at $x = 0$ have terms with negative exponent.

Let the Puiseux expansion $y(x)$ be represented by

$$y(x) = \sum_{k=1}^{\infty} a_k x^{\gamma_1 + \cdots + \gamma_k}, \tag{3.1}$$

where $a_k \neq 0$ for all $k \geq 1$. For $k \geq 1$, let $y_k(x)$ denote the partial sum

$$y_k(x) = \sum_{i=1}^{k} a_i x^{\gamma_1 + \cdots + \gamma_i}, \tag{3.2}$$

and define $y_0(x) = 0$. Let $\gamma_i = e_i/f_i$, with $e_i, f_i \in \mathbf{Z}$, $e_i \geq 1$, and $\gcd(e_i, f_i) = 1$. Let $E_i = \operatorname{lcm}(e_1, \ldots, e_i)$ for $i \geq 1$.

Let T be the number of nonzero terms in the singular part of $y(x)$, then $y_T(x)$ is the singular part of $y(x)$, and no more than $T \leq 4mn^2$ iterations of the procedure described below are required to compute the singular part of $y(x)$.

For $k \geq 1$, α_{k-1} will denote an algebraic integer with the property that $\mathbf{Q}(\alpha_{k-1}) = \mathbf{Q}(a_1, \ldots, a_{k-1})$. Also, for $k \geq 1$ and $0 \leq i \leq k-1$, we define $P_{i,k-1}(x) \in \mathbf{Q}[x]$

with $\deg_x P_{i,k-1} < [\mathbf{Q}(\alpha_k)\colon \mathbf{Q}]$ such that $a_i = P_{i,k-1}(\alpha_{k-1})$. For $k \geq 1$, the polynomial $F_{k-1}(x,y) \in \mathbf{Q}[x^{1/E_{k-1}}, y]$ is defined as

$$F_{k-1}(x,y) = x^{-\beta_1-\cdots-\beta_{k-1}} F(x, x^{\gamma_1+\cdots+\gamma_{k-1}}(y+a_{k-1}) + x^{\gamma_1+\cdots+\gamma_{k-2}} a_{k-2} + \cdots + x^{\gamma_1} a_1),$$

where the segment on the Newton polygon chosen during stage i of the Newton polygon process lies on the line $y + \gamma_i x = \beta_i$ for $i = 1, \ldots, k-1$.

Finally, let $a_0 = \alpha_0 = 1$, $F_0(x,y) = F(x,y)$, and $A_{0,i}(x) = A_i(x)$ for $0 \leq i \leq n$.

Input into Iteration k of Algorithm 1 ($k \geq 1$)**.**

i. $P_{\alpha_{k-1}}(x)$, the minimal polynomial over $\mathbf{Q}$ of α_{k-1}.
ii. The polynomials $P_{i,k-1}(x)$ for $i = 1, \ldots, k-1$.
iii. $P_{a_i}(x)$, the minimal polynomial over $\mathbf{Q}$ of a_i, for $i = 1, \ldots, k-1$.
iv. Nonnegative rational numbers $\gamma_1, \ldots, \gamma_{k-1}$ in reduced form and nonnegative integers $\beta_1, \ldots, \beta_{k-1}$.
v. The polynomial $F_{k-1}(x,y)$ given in the form
$$F_{k-1}(x,y) = A_{k-1,n}(x)y^n + \cdots + A_{k-1,0}(x),$$
where $A_{k-1,i}(x) \in \mathbf{Q}(\alpha_{k-1})[x^{1/E_{k-1}}]$ for $0 \leq i \leq n$.

Output from Iteration k of Algorithm 1.

i. An algebraic integer α_k such that $\mathbf{Q}(\alpha_k) = \mathbf{Q}(a_1, \ldots, a_k)$, defined over $\mathbf{Q}$ by its minimal polynomial $P_{\alpha_k}(x)$.
ii. Polynomials $P_{i,k}(x) \in \mathbf{Q}[x]$ with $\deg_x P_{i,k} < [\mathbf{Q}(\alpha_k)\colon \mathbf{Q}]$ and $a_i = P_{i,k}(\alpha_k)$ for $1 \leq i \leq k$.
iii. The coefficient a_k, defined over $\mathbf{Q}$ by its minimal polynomial $P_{a_k}(x)$.
iv. The rational numbers $\gamma_1, \ldots, \gamma_k$, and the integers $\beta_1, \ldots, \beta_k$.
v. The polynomial $F_k(x,y) = x^{-\beta_k} F_{k-1}(x, x^{\gamma_k}(y+a_k))$ in the form
$$F_k(x,y) = A_{k,n}(x)y^n + \cdots + A_{k,0}(x).$$
vi. The kth partial sum of $y(x)$, which is $y_k(x) = \sum_{i=1}^{k} a_i x^{\gamma_i+\cdots+\gamma_i}$.

Algorithm 1.

Step 1. For each i with $0 \leq i \leq n$, such that $A_{k-1,i}(x) \neq 0$, compute $\alpha_{k-1,i}$, which is defined to be the highest power of x dividing $A_{k-1,i}(x)$. For $i = 0, \ldots, n$ with $A_{k-1}(x) \neq 0$, put $X_{k-1,i} = (i, \alpha_{k-1,i})$ and compute the equations of all lines $L_1, \ldots, L_{s_k}$ which are segments of the lower convex polygon determined by the $X_{k-1,i}$.

Step 2. If $k = 1$ choose any line L_j. If $k > 1$ choose any line L_j with negative slope. Let $y + \gamma_k x = \beta_k$ be the equation of this line. Let G_k denote the set of indices i for which $X_{k-1,i}$ lies on L_j, and put

$$P_k(x) = \left(\sum_{i \in G_k} a_{k-1,i} x^i \right) x^{-l_k},$$

where $a_{k-1,i}$ is the coefficient of $x^{\alpha_{k-1,i}}$ in $F_{k-1}(x,y)$, and $l_k \in \mathbf{Z}$ is chosen so that $P_k(0) \neq 0$ and $P_k(x) \in \mathbf{Q}[\alpha_{k-1}][x]$. Write $P_k(x) = p_{k,d_k}(\alpha_{k-1})x^{d_k} + \cdots + p_{k,0}(\alpha_{k-1})$, where $d_k = \deg_x P_k(x)$, $p_{k,j}(x) \in \mathbf{Q}[x]$ and $\deg_x p_{k,j}(x) < [\mathbf{Q}(\alpha_{k-1})\colon \mathbf{Q}]$ for $0 \leq j \leq d_k$.

Step 3. Compute

$$N = \mathrm{NORM}_{\mathbf{Q}(\alpha_{k-1})/\mathbf{Q}}(p_{k,d_k}(\alpha_{k-1}))$$

by

$$N = \mathrm{res}_x(P_{\alpha_{k-1}}(x), p_{k,d_k}(x)),$$

and then compute $q_k(x) \in \mathbf{Q}[x]$ with $\deg_x q_k(x) < [\mathbf{Q}(\alpha_{k-1})\colon \mathbf{Q}]$ such that

$$q_k(\alpha_{k-1}) \cdot p_{k,d_k}(\alpha_{k-1}) = N.$$

Finally, compute the monic polynomial $P_k^*(x) = (q_k(\alpha_{k-1})/N) \cdot P_k(x)$.

Step 4. Factor $P_k^*(x)$ in $\mathbf{Q}[\alpha_{k-1}][x]$, and choose any irreducible factor $\widetilde{P}_{a_k}$, which defines a new algebraic number a_k over $\mathbf{Q}(\alpha_{k-1})$.

Step 5. Determine if $(\widetilde{P}_{a_k})^2$ divides $P_k^*(x)$ in $\mathbf{Q}[\alpha_{k-1}][x]$. If it does not, then $k = T$, the number of nonzero terms in the singular part of $y(x)$.

Step 6. Compute P_{a_k} by the following steps:

i. Compute $R_k(x) = \mathrm{res}_t(P_{\alpha_{k-1}}(t), \widetilde{P}_{a_k}(x,t))$, where $\widetilde{P}_{a_k}(x,t)$ is obtained from $\widetilde{P}_{a_k}(x)$ by replacing α_{k-1} by t.
ii. Compute $R_k^*(x) = \frac{R_k(x)}{\gcd(R_k, R_k')}$.
iii. Compute $C_k \in \mathbf{Q}$ so that $C_k R_k^*(x) \in \mathbf{Z}[x]$ and is primitive. Then $P_{a_k}(x) = C_k R_k^*(x)$.

Step 7. Put $B_k = \mathrm{lc}(P_{a_k})$, and $\overline{a}_k = B_k a_k$, so that $\overline{a}_k$ is an algebraic integer. Put $r_k = \deg_x P_{a_k}$ and compute $P_{\overline{a}_k} = B_k^{r_k - 1} P_{a_k}(x/B_k)$.

Step 8. If $\widetilde{P}_{a_k}$ is linear, put $\alpha_k = \alpha_{k-1}, t_k = 0$, and $P_{i,k}(x) = P_{i,k-1}(x)$ for $1 \le i \le k-1$. Define $P_{k,k}(x)$ by $a_k = P_{k,k}(\alpha_{k-1})$, where $\widetilde{P}_{a_k} = x - a_k \in \mathbf{Q}[\alpha_{k-1}][x]$, and then proceed to Step 11. If $\widetilde{P}_{a_k}$ is not linear, then proceed to Step 9.

Step 9. Compute a new algebraic integer α_k, given by

$$\alpha_k = \alpha_{k-1} + t_k \overline{a}_k, \quad t_k \in \mathbf{Z},$$

where t_k is chosen such that $\mathbf{Q}(\alpha_k) = \mathbf{Q}(a_1, \ldots, a_k)$ by the following steps.

i. Factor $P_{\overline{a}_k}$ into irreducible factors in $\mathbf{Q}[\alpha_{k-1}][x]$.
ii. For each irreducible factor $q(x)$ obtained with $\deg_x q(x) = \deg_x \widetilde{P}_{a_k}$, determine if $(\frac{\mathrm{lc}(\widetilde{P}_{a_k}) q(B_k x)}{B_k^{\deg_x q(x)}}) = \widetilde{P}_{a_k}(x)$. If so, then $q(x) = \widetilde{P}_{\overline{a}_k}(x)$, the defining polynomial of $\overline{a}_k$ over $\mathbf{Q}(\alpha_{k-1})$.
iii. For $t = 1, 2, \ldots, n^2$ compute $r(x,t) = \mathrm{res}_y(x - y - \alpha_{k-1}, t^{r_k} \widetilde{P}_{\overline{a}_k}(y/t))$. Choose t_k so that $\deg_x r(x, t_k) = \max_{1 \le t \le n^2}\{\deg_x r(x,t)\}$, and put $\alpha_k = \alpha_{k-1} + t_k \overline{a}_k$. Put $\widetilde{P}_{\alpha_k}(x) = r(x, t_k)$, a defining polynomial of α_k over $\mathbf{Q}(\alpha_{k-1})$. By the result in [21, p. 139], α_k is a primitive element of $\mathbf{Q}(a_1, \ldots, a_k)$.
iv. Compute $P_{\alpha_k}(x)$ by the following steps:
   a. Compute $S_k(x) = \mathrm{res}_t(P_{\alpha_{k-1}}(t), \widetilde{P}_{\alpha_k}(x,t))$, where $\widetilde{P}_{\alpha_k}(x,t)$ is obtained from $\widetilde{P}_k(x)$ by replacing α_{k-1} by t.
   b. Compute $S_k^*(x) = \frac{S_k(x)}{\gcd(S_k, S_k')}$.
   c. Compute $D_k \in \mathbf{Z}$ so that $D_k S_k^*(x) \in \mathbf{Z}[x]$ and is primitive. Then $P_{\alpha_k}(x) = D_k S_k^*(x)$.

Step 10. Represent $\overline{a}_1, \ldots, \overline{a}_k$ in $\mathbf{Q}(\alpha_k)$ by the following steps:

i. Compute $\gcd_{\mathbf{Q}(\alpha_k)}(P_{\alpha_{k-1}}(\alpha_k - t_k x), P_{\overline{a}_k}(x)) = x - \overline{a}_k \in \mathbf{Q}[\alpha_k][x]$ to obtain $\overline{a}_k = P^*_{k,k}(\alpha_k)$. Put $P_{k,k}(x) = (\frac{1}{B_k})P^*_{k,k}(x)$.

ii. For each i with $1 \le i \le k-1$, the following steps:

   a. Factor $P_{\overline{a}_i}(x)$ into irreducible factors in $\mathbf{Q}[\alpha_k][x]$.

   b. Put $Q_{i,k}(x) = P_{i,k-1}(x - t_k B_k P_{k,k}(x))$ so that $a_i = Q_{i,k}(\alpha_k)$.

   c. For each monic linear factor $x - Q(\alpha_k)$ of $P_{\overline{a}_i}(x)$ obtained in a (above), check if $P_{\alpha_k}(x)$ divides $Q(x) - B_i Q_{i,k}(x)$ in $\mathbf{Q}[x]$. If so, then put $P_{i,k}(x) = \frac{1}{B_i}Q(x)$.

Step 11. Put $y_k(x) = a_1 x^{\gamma_1} + \cdots + a_k x^{\gamma_1 + \cdots + \gamma_k}$ and compute

$$F_k = x^{-\beta_k} F_{k-1}(x, x^{\gamma_k}(y + a_k))$$

in the form

$$F_k(x, y) = A_{k,n}(x) y^n + \cdots + A_{k,0}(x)$$

with $a_1, \ldots, a_k \in \mathbf{Q}(\alpha_k)$, and $A_{k,n}(x), \ldots, A_{k,0}(x) \in \mathbf{Q}(\alpha_k)[x]$. Let $k = k + 1$.

4. Complexity of Algorithm 1

The purpose of this section is to compute an estimate for the number of bit operations required to compute the singular part of a Puiseux expansion at $x = 0$ of the algebraic function y defined by $F(x, y) = 0$, with $F(x, y)$ in (2.1). This is accomplished by first proving estimates for the size of the quantities appearing in Algorithm 1 and then performing a complexity analysis on each step in Algorithm 1.

Lemma 4.1. *Let $P(x) = a_n(\alpha)x^n + \cdots + a_0(\alpha) \in \mathbf{Z}[\alpha][x]$, where α is an algebraic integer of degree d over $\mathbf{Q}$ and height h, and put $N = N_{\mathbf{Q}(\alpha)/\mathbf{Q}}(a_n(\alpha))$. Put $A = \mathrm{ht}(a_n(x))$ and let $Q(x) \in \mathbf{Q}[x]$ be the polynomial which satisfies $\deg_x Q(x) \le d - 1$ and $Q(\alpha)a_n(\alpha) = N$. Then the following inequalities hold:*

i. $|N| \le (dhA)^d$;

ii. $\mathrm{ht}(Q) \le d^{(5d-3)/2}(h+1)^{d(d+1)/2}A^{(3d-1)/2}$;

iii. $\mathrm{denom}(Q) \le d^{4d}(h+1)^{d^2+d}A^{2d}$.

Proof. By [16, Theorem 1], $N = \mathrm{res}_t(a_n(t), P_\alpha(t))$, and so by Hadamard's determinantal inequality (for example, see [9, 1.3(v)]),

$$|N| \le \left(\prod_{i=1}^{d} dh^2\right)^{1/2} \left(\prod_{i=1}^{d} dA^2\right)^{1/2} = (dhA)^d.$$

Let $Q(\alpha) = x_{d-1}al^{d-1} + \cdots + x_0$ and $a_n(\alpha) = A_{d-1}x^{d-1} + \cdots + A_0$, so that

$$x_{d-1}A_{d-1}\alpha^{2d+2} + \cdots + (x_j A_0 + \cdots + x_0 A_j)\alpha^j + \cdots + x_0 A_0 = N. \tag{4.1}$$

Equation (4.1) yields d linear equations in the d unknowns $x_0, \ldots, x_{d-1}$. By replacing each power α^j, with $j < d-1$, in (4.1) by its unique representation as a linear combination of $1, \alpha, \ldots, \alpha^{d-1}$, and collecting terms, one obtains by Cramer's Rule that

$$x_i = \frac{\det(M_i)}{\det(M)}, \quad 0 \le i \le d-1, \tag{4.2}$$

where M is the resulting matrix of the system, and M_i is obtained from M by replacing column $i+1$ of M by the column with N in the last entry and zeros elsewhere. By a simple inductive argument it is easy to prove that

$$(\alpha^t)_{\max} \leq h(h+1)^{t-n} \tag{4.3}$$

for all $t \geq n$. Therefore, each entry of M is a rational number whose absolute value is no larger than $(h+1)^{d-1}d^2A$. The same bound holds for all entries of M_i, except for the lone entry of N in position (i,d). Thus, by part (i) above and Hadamard's inequality,

$$|x_i| \leq (dhA)^d \left(\prod_{i=1}^{d-1} dd^2(h+1)^d A\right)^{1/2} \leq d^{(5d-3)/2}(h+1)^{d(d+1)/2}A^{(3d-1)/2},$$

and

$$\operatorname{denom}(Q) = \max_{0\leq i\leq d-1}\{\operatorname{denom}(x_i)\} \leq \det M \cdot \det M_i \leq d^{4d}(h+1)^{d^2+d}A^{2d}.$$

Lemma 4.2. *Let $P(x) = \sum_{i=0}^n a_i(\alpha)x^i \in \mathbf{Q}[\alpha][x]$, where α is an algebraic number of degree d and height h, and $\deg_x a_i(x) \leq d-1$ for $0 \leq i \leq n$. Let $Q(\alpha)$ and N be as in Lemma 4.1, and define*

$$P^*(x) = \frac{Q(\alpha)}{N}P(x).$$

Then

$$(P^*)_{\max} \leq d^{3d}(h+1)^{d^2}P_{\max}^{2d}$$

and

$$\operatorname{denom}(P^*) \leq N \cdot \operatorname{denom}(Q) \cdot \operatorname{denom}(P).$$

Proof. From the definition of P^* it is evident that

$$\operatorname{denom}(P^*) \leq N \cdot \operatorname{denom}(Q) \cdot \operatorname{denom}(P).$$

For $0 \leq i \leq n$, $Q(\alpha)a_i(\alpha)$ is an expression of the form described in (4.1). From (4.1) and (4.3) we deduce that

$$\begin{aligned}(P^*)_{\max} &\leq d^2 Q_{\max}P_{\max} \cdot \max_{1\leq j\leq d-2}\operatorname{ht}(\alpha^j)\\ &\leq d^2 d^{(5d-3)/2}(h+1)^{d(d+1)/2}(P_{\max})^{(3d-1)/2}h(h+1)^{d-1}\\ &\leq d^{3d}(h+1)^{d^2}P_{\max}^{2d}.\end{aligned}$$

Lemma 4.3. *Let all of the notation be as in Algorithm 1. Also, let*

$$A = \max_{1\leq k\leq T}\{\|a_k\|\} \quad \textit{and} \quad B = \max_{1\leq k\leq T}\{B_k\}.$$

1. $\operatorname{ht}(P_{\alpha_k}) \leq (8n^4mBA)^n$ *for* $1 \leq k \leq T$.
2. $\operatorname{ht}(P_{\overline{a}_k}) \leq (2BA)^n$ *for* $1 \leq k \leq T$.
3. $\operatorname{ht}(P_{a_k}) \leq B(2A)^n$ *for* $1 \leq k \leq T$.
4. $\log(\operatorname{ht}(P_{i,k})) = O(n^2\log(nmBA))$ *for* $1 \leq k \leq T$ *and* $1 \leq i \leq k$.
5. $\log((P_k)_{\max}) = O(n^2\log(nmBA))$ *for* $1 \leq k \leq T$.
6. $\log((P_k^*)_{\max}) = O(n^3\log(nmBA))$ *for* $1 \leq k \leq T$.
7. $\log(\operatorname{denom}((P_k^*)_{\max})) = O(n^3\log(nmBA))$ *for* $1 \leq k \leq T$.
8. $\log((\widetilde{P}_{a_k})_{\max}) = O(n^2\log(nmBA))$ *for* $1 \leq k \leq T$.
9. $\log(\operatorname{ht}(R_k)) = O(n^3\log(nmBA))$ *for* $1 \leq k \leq T$.

10. $\log(\mathrm{denom}(R_k^*)) = O(n^3 \log(nmBA))$ *for* $1 \le k \le T$.
11. $\log(\mathrm{ht}(\mathrm{denom}((R_k^*) \cdot R_k^*))) = O(n^3 \log(nmBA))$ *for* $1 \le k \le T$.
12. $\log((\widetilde{P}_{\overline{a_k}}) = O(n^2 \log(nmBA))$ *for* $1 \le k \le T$.

Proof.

1. $\mathrm{ht}(P_{\alpha_k}) \le \mathrm{ht}(\prod_{i=1}^n x + \|\alpha_k\|) \le 2^n \|\alpha_k\|^n$, and the result follows from the bound $\|\alpha_k\| = \|B_1 a_1 + t_1 B_2 a_2 + \cdots + t_{k-1} B_k a_k\| \le TBAn^2 \le 4n^4 mBA$.

2. $\mathrm{ht}(P_{\overline{a}_k}) \le \mathrm{ht}(\prod_{i=1}^n (x + \|\overline{a_k}\|)) \le 2^n B^n A^n$.

3. $\mathrm{ht}(P_{a_k}) \le \mathrm{ht}(B_k \cdot \prod_{i=1}^n (x + \|a_k\|)) \le B(2A)^n$.

4. From the bound in Theorem B with $f(x) = P_{\overline{a}_i}(x)$, $\alpha = \alpha_k$, and $h(x) = x - \overline{a}_i \in \mathbf{Q}[\alpha_k][x]$, we obtain

$$\begin{aligned}\mathrm{ht}(P_{i,k}) &\le B \cdot \mathrm{ht}(P_{\overline{a}_i})(2(n+1)^2 n^3 n^n \cdot 2)^{1/2} |P_{\alpha_k}|^{2n} \\ &\le 2^n B^{n+1} A^n (2(n+1)^2 n^3 n^n \cdot 2)^{1/2} (\sqrt{n})^{2n}\, \mathrm{ht}(P_{\alpha_k})^{2n},\end{aligned}$$

and the result follows from Lemma 4.3 1 above and taking the logarithm of the result.

5. We have, from the input into Algorithm 1,

$$\begin{aligned}F_{k-1}(x,y) &= x^{-\beta_1-\beta_2-\cdots-\beta_{k-1}} F(x, x^{\gamma_1+\gamma_2+\cdots+\gamma_{k-1}}(y + a_{k-1}) + \cdots + x^{\gamma_1} a_1) \\ &= x^{-\beta_1-\beta_2-\cdots-\beta_{k-1}} \Bigg[A_n(x) \Bigg(x^{(\gamma_1+\gamma_2+\cdots+\gamma_{k-1})n} \Bigg(y + \frac{P_{k-1,k-1}(\alpha_{k-1})}{B_{k-1}} \Bigg)^n \Bigg) \\ &\qquad + \cdots + x^{\gamma_1 n} \Bigg(\frac{P_{1,k-1}(\alpha_{k-1})}{B_1} \Bigg)^n + \cdots + A_0(x) \Bigg].\end{aligned}$$

Therefore, since $(P_k)_{\max} \le (F_{k-1})_{\max}$, we have that

$$\begin{aligned}(P_k)_{\max} &\le (n+1)(2nm)(n+1)(n+1)^n \\ &\qquad \cdot 2^n \cdot h \cdot \max_{1 \le j \le k-1} \{((P_{j,k-1}(\alpha_{k-1}))^n)_{\max}\} \\ &\le n^{n+3} 2^{2n+2} m \cdot h \cdot (\max_{1 \le j \le k-1} \{\mathrm{ht}(P_{j,k-1}(x))\})^n \\ &\qquad \cdot \mathrm{ht}((1 + \cdots + \alpha^{n-1})^n) \\ &\le n^{n+3} 2^{2n+2} mh (\max_{1 \le j \le k-1} \{\mathrm{ht}(P_{j,k-1}(x))\})^n \\ &\qquad \cdot n^{n+2} \max_{1 \le l \le n} \{\mathrm{ht}(\alpha^l)\}.\end{aligned}$$

The result now follows by taking the logarithm of this last estimate, and then applying Lemma 4.1 along with the bound in Lemma 4.3 4 for $\log(\mathrm{ht}(P_{i,k}))$ given above.

6.

$$\begin{aligned}(P_k^*)_{\max} &\le \mathrm{ht}(q_k) \cdot (P_k)_{\max} \cdot n^2 \cdot \max_{1 \le l \le 2n} \{\mathrm{ht}(\alpha^l)\} \\ &\le n^{3n} (\mathrm{ht}(P_{\alpha_{k-1}}) + 1)^{n(n+1)/2} (P_k)_{\max}^{3n} \cdot n^2 \cdot \mathrm{ht}(P_{\alpha_{k-1}})^{n+1} \\ &\le n^{3n+2} (\mathrm{ht}(P_{\alpha_{k-1}}) + 1)^{2n^2} (P_k)_{\max}^{3n}.\end{aligned}$$

The result follows by using Lemma 4.3 1 above, taking the logarithm of this last estimate, and using the bound obtained in Lemma 4.3 5 for $(P_k)_{\max}$.

7.

$$\begin{aligned}\operatorname{denom}(P_k^*) &\le N \cdot \operatorname{denom}(q_k(x)) \cdot \operatorname{denom}(P_k)\\ &\le (n \operatorname{ht}(\alpha_{k-1})(P_k)_{\max})^n (n^{4n}(\operatorname{ht}(P_{\alpha_{k-1}})+1)^{n^2+n} \cdot (P_k)_{\max}^{2n})^{1/2} \cdot B^n\\ &\le n^{3n} B^n (\operatorname{ht}(P_{\alpha_{k-1}})+1)^{n(n+3)/2} (P_k)_{\max}^{2n}.\end{aligned}$$

The result follows by using Lemma 4.3 1, taking the logarithm of this last estimate, and using the bound obtained in Lemma 4.3 5 for $(P_k)_{\max}$.

8. Applying the bound in Theorem B to $f = \frac{1}{\operatorname{lc}(P_{a_k})} \cdot P_{a_k}$, with $\alpha = \alpha_{k-1}$, one obtains

$$(\widetilde{P}_{a_k})_{\max} \le \operatorname{ht}(P_{a_k})(2(n+1)^2 n^3 n^n 2^{2n})^{1/2} \operatorname{ht}(P_{\alpha_{k-1}})^{2n} n^n.$$

The result follows by applying Lemma 4.3 1 and 3, along with taking the logarithm of this last estimate.

9. From the definition of resultant, we obtain the estimate

$$\begin{aligned}\operatorname{ht}(R_k(x)) &\le (2n)^{2n} \operatorname{ht}(P_{\alpha_k-1})^n (\widetilde{P}_{a_k})_{\max}^n \operatorname{ht}((1+\cdots+x^{n-1})^n)\\ &\le (2n)^{2n} \operatorname{ht}(P_{\alpha_{k-1}})^n (\widetilde{P}_{a_k})_{\max}^n n^n\\ &\le 2^{2n} n^{3n} \operatorname{ht}(P_{\alpha_{k-1}})^n (\widetilde{P}_{a_k})_{\max}^n.\end{aligned}$$

The result now follows by taking the logarithm of this last estimate and using Lemma 4.3 1 and 8.

10. From [20, Theorem 2.1], there is a positive integer r and $u/v \in \mathbf{Q}$ such that $R_k(x) = (u/v)P_{a_k}^r$. Therefore, since $R_k'(x) = (ru/v)P_{a_k}^{r-1}P_{a_k}'$, and $\gcd(R_k, R_k') = \frac{(P_{a_k})^{r-1}}{\operatorname{lc}((P_{a_k})^{r-1})}$, it follows that $R_k^*(x) = (u/v)\frac{1}{\operatorname{lc}((P_{a_k})^{r-1})}P_{a_k}$. Therefore $\operatorname{denom}(R_k^*) \le \operatorname{ht}(P_{a_k})^n \operatorname{denom}(R_k)$, and once again using Theorem B we obtain,

$$\operatorname{denom}(R_k(x)) \le (\operatorname{denom}(\widetilde{P}_a))^n \le (\operatorname{ht}(P_{a_k}) \cdot \operatorname{disc}(P_{\alpha_{k-1}}))^n.$$

We now estimate $\operatorname{disc}(P_{\alpha_k})$, for $1 \le k \le T$. Note that $\operatorname{disc}(P_{\alpha_k}) = \operatorname{res}_x(P_{\alpha_k}, P_{\alpha_k}')$, and so by Hadamard's inequality and Lemma 4.3 1, $\operatorname{disc}(P_{\alpha_k}) \le (n \cdot \operatorname{ht}(P_{\alpha_k}))^n \le n^n(4n^3mBA)^{n^2}$. The result now follows by combining the above estimates, applying the estimate in Lemma 4.3 1, and taking the logarithm of the result.

11. From the argument in Lemma 4.3 10 $R_k^* = (u/v)\frac{1}{(\operatorname{lc}(P_{a_k}))^{r-1}}P_{a_k}$, and so $(\operatorname{denom}(R_k^*)) \cdot R_k^* = uP_{a_k}$. Therefore,

$$\begin{aligned}u \le \operatorname{lc}(u \cdot P_{a_k}) &= \operatorname{lc}(\operatorname{denom}((R_k^*) \cdot R_k^*))\\ &= \operatorname{denom}(R_k^*) \cdot \operatorname{lc}(R_k^*)\\ &= \operatorname{denom}(R_k^*) \cdot \operatorname{lc}(R_k)\\ &\le \operatorname{denom}(R_k^*) \cdot \operatorname{ht}(R_k).\end{aligned}$$

Therefore, $\operatorname{ht}(\operatorname{denom}(R_k^*) \cdot R_k^*) = u \cdot \operatorname{ht}(P_{a_k}) \le \operatorname{denom}(R_k^*) \operatorname{ht}(R_k) \operatorname{ht}(P_{a_k})$. The result now follows from Lemma 4.3 10, 9, 3, and taking the logarithm of both sides of this last estimate.

12. This is another application of Theorem B, with $f = P_{\overline{a_k}}$ and $\alpha = \alpha_{k-1}$.

Lemma 4.4. *Let $M = (m_{i,j})$ be an $n \times n$ matrix with entries that are polynomials with integer coefficients in t variables $x_1, \ldots, x_t$ such that $\deg_{x_k} m_{i,j} \leq d$ for $1 \leq k \leq t$ and $\mathrm{ht}(m_{i,j}) \leq h$ for all $1 \leq i, j \leq n$. Given any $\varepsilon > 0$, the number of bit operations needed to compute the determinant of M is*

$$O(n^{4+\varepsilon}(\log^{1+\varepsilon}(dh))(dn+1)^{2t}).$$

Proof. If $W(L, D, H)$ denotes the number of bit operations required to multiply two rational polynomials in L variables of degrees bounded by D in each variable, and height bounded by H, then $W(L, D, H) = O((D+1)^{2L} \log^{1+\varepsilon}(H))$. To see this, observe that the polynomials being multiplied are the sum of at most $(D+1)^L$ monomials, and hence the overall work requires at most $(D+1)^{2L}$ multiplications on integers whose absolute value is bounded by H, and then some additions to recover the product. The multiplications dominate the overall complexity, and so the result follows from the fact that a multiplication on two integers of size k bits each requires at most $O(k^{1+\varepsilon})$ bit operations.

If the first column of M is all zero, then $\det(M) = 0$. Otherwise, $O(n^2 W(t, d, h))$ bit operations are required to produce a nonzero element in the first row of this column, and zeros below. Similarly, for column i, either the entire column is zero, in which case $\det(M) = 0$, or else $O((n+1-i)^2 W(t, id, d^{i-1}h^i))$ bit operations suffice to produce a nonzero element in position (i, i) of the matrix, and zeros below. The work to multiply the diagonal of the resulting upper-triangular matrix is no greater than the work performed in producing the upper-triangular form, and so the total work is $O(n^3 W(t, nd, (dh)^n))$. The result now follows from the estimate given above for $W(L, D, H)$.

Proof of Theorem 1. In this analysis, we will use the fact that given any $\varepsilon > 0$ an arithmetic operation on two integers of size k bits each requires at most $O(k^{1+\varepsilon})$ bit operations. We will also assume that the iteration being performed is computing a term in the singular part of $y(x)$. In other words, we will assume that $k \leq T$, and so $k \leq 4mn^2$.

The work in Step 1 is the computation of the equations of at most n lines, each one determined by a pair of points $X_{k-1,i}$ and $X_{k-1,j}$. The coordinates of these points are integers whose absolute value does not exceed $kn^2 + m$. This bound follows from the fact that $\deg_y F_k = n$ and $\deg_x F_k \leq m + \sum_{i=1}^{k} \gamma_i n$ for all $k \geq 0$, together with the estimate $\gamma_k \leq n$ for each $k \geq 1$. Since we are assuming that $k \leq 4mn^2$, the number of bit operations required to complete Step 1 is therefore $O(n \log^{1+\varepsilon}(nm))$ for any $\varepsilon > 0$.

The work required to perform Step 2 is to write down the polynomial $P_k(x)$ in $\mathbf{Q}[\alpha_{k-1}][x]$. The number of bit operations required is $O(\log((P_k)_{\max}))$, which by part 5 of Lemma 4.3 is $O(n^2 \log(nmBA))$.

The work required in the first part of Step 3 is the computation of at most $n+1$ determinants of matrices of size no larger than $2n$, whose entries are polynomials in one variable, with rational coefficients, of degree bounded by n, and of height bounded by $(P_k)_{\max}$. By part 5 of Lemma 4.3 and Lemma 4.4, the number of bit operations required is $O(n^{9+\varepsilon} \log^{1+\varepsilon}(nmBA))$.

We remark here that, as a consequence of [10, Theorem A, p. 260], the number of bit operations required to multiply two polynomials, f and g, with rational coefficients, and of height bounded by a number H is $O(\deg(f) \cdot \deg(g) \cdot \log^{1+\varepsilon}(H))$.

The work in the latter part of Step 3 involves multiplying $q_k(\alpha_{k-1})/N$ to each coefficient of $P_k(x)$. By Lemma 4.1, parts 1 and 5 of Lemma 4.3, and the above observation regarding the number of bit operations needed to multiply polynomials, we get that the number of bit operations required for Step 3 is

$$\begin{aligned} &O(n \cdot n^2 \cdot \log^{1+\varepsilon}(\mathrm{ht}(q_k(x)))) \\ &\quad = O(n^3 \cdot \log^{1+\varepsilon}(n^{3n}\, \mathrm{ht}(P_{\alpha_{k-1}})^{2n^2}(P_k)_{\max})) \\ &\quad = O(n^{5+\varepsilon} \cdot \log^{1+\varepsilon}(n \cdot \mathrm{ht}((P_{\alpha_{k-1}}) \cdot (P_k)_{\max}))) \\ &\quad = O(n^{7+\varepsilon} \cdot \log^{1+\varepsilon}(nmBA)). \end{aligned}$$

By Theorem B the number of arithmetic operations required to perform Step 4 is $O(n^{10} \log(\mathrm{denom}(P_k^*) \cdot (P_k^*)_{\max}))$, which, by parts 6 and 7 of Lemma 4.3, is $O(n^{13} \log(nmBA))$. The size of the integers on which these oprations are performed are $O(n^4 \log(\mathrm{denom}(P_k^*) \cdot (P_k^*)_{\max}))$, which is $O(n^7 \log(nmBA))$. Therefore, the number of bit operations required to complete Step 4 is

$$O(n^{20+\varepsilon} \log^{2+\varepsilon}(nmBA)). \tag{4.4}$$

Note that this complexity bound dominates the complexity bounds of all of the previous steps.

The work in Step 5 involves at most n equality tests with $\widetilde{P}_{a_k}$ and the other factors of $P_k^*(x)$ in $\mathbf{Q}[\alpha_{k-1}][x]$. By parts 6 and 8 of Lemma 4.3, the number of bit operations required is $O(n^4 \cdot \log(nmBA))$, which is dominated by the bound in (4.4).

The work involved in Step 6.i is the computation of a determinant of a matrix whose dimensions are at most $2n \times 2n$, and whose entries are polynomials in 2 variables, of degree bounded by n, and height bounded by

$$h_1 = \max\{\mathrm{ht}((P_{\alpha_{k-1}}), (\widetilde{P}_{a_k})_{\max})\}.$$

Therefore, by parts 1 and 8 of Lemma 4.3, and Lemma 4.4, the number of bit operations required is $O(n^{14+\varepsilon} \cdot \log^{1+\varepsilon}(nmBA))$. Note that this work factor is dominated by that in (4.4).

By part 1 of Theorem C, the number of bit operations required to compute $\gcd(R_k, R_k')$ in Step 6.ii, is $O(\max\{\log(|R_k|, \log|R_k'|)\}^2 \cdot \max\{\deg(R_k), \deg(R_k')\}^4)$. From the definition of R_k, we have $\deg(R_k') \le \deg(R_k) \le n^2$. This is the dominant part of Step 6.ii, and we simplify the above expression to find that Step 6.ii can be completed in $O(n^{11} \cdot \log^2(\mathrm{ht}(R_k)))$ bit operations. By part 9 of Lemma 4.3, this is equal to $O(n^{17} \cdot \log^2(nmBA))$ bit operations. Note that this complexity bound is dominated by that in (4.4).

Step 6.iii is accomplished by first multiplying $R_k^*(x)$ by its denominator, and then dividing the resulting polynomial, $\mathrm{denom}(R_k^*) \cdot R_k^*$, by its content. By part 10 of Lemma 4.3, multiplying $R_k^*(x)$ by its denominator requires $O(n^{4+\varepsilon} \cdot \log^{1+\varepsilon}(nmBA))$ bit operations. We now estimate the number of bit operations required to compute the content of $\mathrm{denom}(R_k^*) \cdot R_k^*$. Since $\deg R_k = \deg P_{a_k} \le n$, this involves computing no more than n greatest common divisors, each one involving integers bounded by $\mathrm{ht}(\mathrm{denom}(R_k^*) \cdot R_k^*)$. By the Euclidean algorithm, for any $\varepsilon > 0$, the work to compute the greatest common divisor of two k-bit integers is $O(\log^{2+\varepsilon}(k))$ bit operations. Therefore, by part 11 of Lemma 4.3, the number of bit operations required for

Step 6.iii is

$$O(n \cdot \log^{2+\varepsilon}(\mathrm{ht}(\mathrm{denom}(R_k^*) \cdot R_k^*))) = O(n^{7+\varepsilon} \cdot \log^{2+\varepsilon}(nmBA)).$$

Note that this complexity bound is dominated by that in (4.4).

The work in Step 7 involves at most $2n$ multiplications involving integers no larger than $B^n \cdot \max\{\mathrm{ht}(P_{a_k}), \mathrm{ht}(P_{k,k-1})\}$. By parts 3 and 4 of Lemma 4.3, the total number of bit operations required is $O(n^{3+\varepsilon} \cdot \log^{1+\varepsilon}(nmBA))$, which is dominated by the complexity bound in (4.4). The work in Step 8 amounts to deciding whether $\widetilde{P}_{a_k}$ is linear or not. This requires a neglible number of bit operations, and so we forgo any analysis of the complexity.

By Theorem B, with $f = P_{\overline{a}_k}$ and $\alpha = \alpha_{k-1}$, the number of arithmetic operations required to factor $P_{\overline{a}_k}$ is $O(n^{11}\log(BA))$, while each operation is performed on integers of size bounded by $O(n^5 \log(BA))$. Thus, the total number of bit operations required to complete Step 9.i is $O(n^{16+\varepsilon} \cdot \log^{2+\varepsilon}(BA))$. This is dominated by the number of bit operations required to complete Step 4. The work to complete Step 9.ii involves at most n equality tests, each test requiring at most n multiplications of integers no larger than $B^n \cdot \max\{(\widetilde{P}_{a_k})_{\max} \mathrm{ht}(P_{\overline{a}_k})\}$, and so by parts 2 and 8 of Lemma 4.3, the number of bit operations required is $O(n^{4+\varepsilon} \cdot \log^{1+\varepsilon}(nmBA))$.

The work in Step 9.iii is the computation of a determinant of a matrix of size no larger than $n+1$ by $n+1$, whose entries are either 0, 1 or $x - \alpha_{k-1}$, except for the bottom row, whose entries consist of the coefficients of $t^{r_k}\widetilde{P}_{\overline{a}_k}(y/t)$, regarded as a polynomial in y. By part 12 of Lemma 4.3, along with Lemma 4.4, the number of bit operations required to compute this determinant is $O(n^{10+\varepsilon} \cdot \log^{1+\varepsilon}(nmBA))$, which is dominated by the bound in (4.4).

Step 9.iv is very similar to Step 6. A similar analysis as that provided for Step 6 shows that the number of bit operations required to complete Step 9.iv is $O(n^{17} \cdot \log^{2+\varepsilon}(nmBA))$, which is dominated by the complexity bound in (4.4).

The dominating part of Step 10.i is the computation of

$$\gcd_{Q(\alpha_k)}(P_{\alpha_k - 1}(\alpha_k - t_k x), P_{\overline{a}_k}(x)).$$

By part 2 of Theorem C, the number of bit operations required is

$$O(n^9 \cdot \log^2(n \cdot \max\{(P_{\alpha_{k-1}}(\alpha_k - t_k x))_{\max}, \mathrm{ht}(P_{\overline{a}_k})\} \cdot \mathrm{ht}(P_{\alpha_k})^n)).$$

From the fact that $t_k \le n^2$, it follows that

$$(P_{\alpha_{k-1}}(\alpha_k - t_k x))_{\max} \le 2^n n^4 \,\mathrm{ht}(P_{\alpha_k})\,\mathrm{ht}(P_{\alpha_{k-1}}),$$

and from parts 1 and 2 of Lemma 4.3, the number of bit operations required to complete this is $O(n^{13} \cdot \log^2(mBA))$, which is dominated by the complexity bound in (4.4).

The only significant amount of work left is in Step 10.ii.a. But this work factor is identical to that in Step 9.i, which is $O(n^{16+\varepsilon} \cdot \log^{2+\varepsilon}(BA))$ bit operations. The completion of Step 10.ii requires no more than $T \le 4mn^2$ iterations of this procedure, and so the total work is

$$O(n^{17+\varepsilon} m \cdot \log^{2+\varepsilon}(BA)). \tag{4.5}$$

The work in Step 11 is essentially writing down $y(x)$ and also computing $F_k(x,y)$. The latter of these two tasks dominates, and it requires on the order of n^3 multiplications of integers no larger than $O(\mathrm{ht}(P_{k,k}(x))^n)$. Therefore, by part 4 of

Lemma 4.3, the number of bit operations required is $O(n^{6+\varepsilon} \cdot \log^{1+\varepsilon}(mBA))$. This is dominated by the complexity bound in (4.4).

By the estimates in (4.4) and (4.5), the number of bit operations required to complete one iteration of Algorithm 1 in $O(n^{20} m \log^{2+\varepsilon}(BA))$.

Let β be an algebraic number. Then β is a root of the integral polynomial $P_{\nu\beta}(\nu x)$, where $\nu = \mathrm{denom}(\beta)$. It follows that $\mathrm{lc}(P_\beta) \leq (\mathrm{denom}(\beta))^{\deg(\beta)}$ for any algebraic number β.

By the remark in the preceding paragraph, the definition of B, and Theorem A we have that

$$\begin{aligned} B &\leq \max_{1\leq k\leq 4mn^2} B_k \\ &\leq \max_{1\leq k\leq 4mn^2} (\mathrm{denom}(a_k))^n \\ &\leq [4.8(8e^{-3} n^{4+2.74\log n} e^{1.22n} h^2 (mn+1)^2)^n]^{4n^3 m}, \end{aligned}$$

and by [18, Lemma 2] (see also [23, Lemma 2.6] or [9, proof of Theorem 3.31]),

$$A \leq 2(h+1)(h(m+1)(n+1))^{6mn^2}.$$

Therefore the number of bit operations to complete one iteration of Algorithm 1 is $O(n^{30+\varepsilon} m^{3+\varepsilon} \cdot \log^{2+\varepsilon}(h))$. Theorem 1 now follows from the fact that $T \leq 4mn^2$, and the fact that T iterations of Algorithm 1 are required to compute the singular part of $y(x)$.

References

[1] G. A. Bliss, *Algebraic Functions*, Amer. Math. Soc. Colloq. Publ. **16** (1933).

[2] W. S. Brown, *On Euclid's algorithm and the computation of polynomial greatest common divisors*, J. Assoc. Comput. Mach., **18** (1971), 478–504. MR **46:**6570

[3] A. L. Chistov, *Polynomial complexity of the Newton-Puiseux algorithm*, Lecture Notes in Computer Sciences, **233** (1986), 247–255. CMP 19:07

[4] D. V. Chudnovsky and G. V. Chudnovsky, *On expansion of algebraic functions in power and Puiseux series* I, J. Complexity, **2** (1986), 271–294. MR **90d:**68031a

[5] ———, *On expansion of algebraic functions in power and Puiseux series* II, J. Complexity, **3** (1987), 1–25. MR **90d:**68031b

[6] J. Coates, *Construction of rational functions on a curve*, Proc. Cambridge Philos. Soc. **68** (1970), 105–123. MR **41:**3477

[7] D. Duval, *Rational Puiseux expansions*, Compositio Math. **70** (1989), 119–154. MR **90c:**14001

[8] B. M. Dwork and A. J. van der Poorten, *The Eisenstein constant*, Duke Math. J. **65**, no. 1 (1992), 23–43. MR **93c:**12010

[9] 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

[10] D. Knuth, *The Art of Computer Programming, vol. II: 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] L. Langemyr, *An analysis of the subresultant algorithm over an algebraic number field*, Proceedings of ISSAC '91, ACM Press, 1991, 167–172.

[14] A. K. Lenstra, *Factoring polynomials over algebraic number fields*, Proc. EuroCal. 1983, Lecture Notes in Computer Science, **162** (1983), 245–254. MR **86d:**12001b

[15] 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] R. Loos, *Computing in algebraic extensions*, in Computer Algebra, 2nd ed., edited by B. Buchberger et. al., Springer-Verlag, New York, 1982, 173–187. CMP 16:06

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

[18] W. M. Schmidt, *Eisenstein's theorem on power series expansions of algebraic functions*, Acta Arith. **56** (1990), 161–179. MR **91m:**11021

[19] J. T. Schwartz and M. Sharir, *On the piano mover's problem*: III, in Planning, Geometry, and Complexity of Robot Motion, edited by J. T. Schwartz, M. Sharir, and J. Hopcroft, Ablex, New York, 1987. MR **86a:**52016

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

[21] B. L. van der Waerden, *Modern Algebra*, Frederick Ungar, 7th ed., New York, 1970. MR **10:**587b

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

[23] P. G. Walsh, *The Computation of Puiseux Expansions and Runge's Theorem on Diophantine Equations*, Ph.D. Thesis, University of Waterloo, Waterloo, Ontario, Canada, 1993.

Department of Mathematics, University of Ottawa, 585 King Edward, Ottawa, Ontario, Canada KIN 6N5

E-mail address: gwalsh@mathstat.uottawa.ca