ALL ALGEBRAIC FUNCTIONS CAN BE COMPUTED FAST*

H. T. Kung and J. F. Traub
Department of Computer Science
Carnegie-Mellon University
Pittsburgh, Pennsylvania 15213

July 1976

*The major results of this paper were announced in the Symposium on Algorithms and Complexity: New Directions and Recent Results, Carnegie-Mellon University, April 7-9, 1976.

This work has been supported in part by the National Science Foundation under Grant MCS 75-222-55 and the Office of Naval Research under Contract N00014-76-C-0370, NR 044-422.

ABSTRACT

The expansions of algebraic functions can be computed "fast" using the Newton Polygon Process and any "normal" iteration. Let M(j) be the number of operations sufficient to multiply two jth degree polynomials. It is shown that the first N terms of an expansion of any algebraic function defined by an nth degree polynomial can be computed in O(n(M(N)) operations, while the classical method needs $O(N^n)$ operations. Among the numerous applications of algebraic functions are symbolic mathematics and combinatorial analysis. Reversion, reciprocation, and nth root of a polynomial are all special cases of algebraic functions.

TABLE OF CONTENTS

1. INTRODUCTION

Let

$$(1.1)\quad P(W,z) = A_n(z)W^n + \ldots + A_0(z),$$

where the $A_i(z)$ are polynomials over a field Δ. In general we shall take Δ to be the field of complex numbers; an exception being Section 7. (Many of the results hold for an algebraically closed field of characteristic 0.) Without loss of generality we assume $A_0(z) \not\equiv 0$ and $A_n(z) \not\equiv 0$. Capital letters will denote polynomials or series; lower case letters will denote scalars.

The zero of (1.1), a function $S(z)$ such that $P(S(z),z) \equiv 0$, is called the algebraic function corresponding to $P(W,z)$. Let z_0 be an arbitrary complex number, finite or infinite. It is known from the general theory of algebraic functions that $S(z)$ has n fractional power series expansions around z_0. By the computation of an algebraic function we shall mean the computation of the first N coefficients (including zero coefficients) of one of its expansions. (This will be made precise in Section 3.) The problem we study in this paper is the computation of one expansion of the algebraic function. Our results can easily be modified for computing more than one expansion or all expansions of the algebraic function.

As described in most texts, the classical method computes algebraic functions by comparison of coefficients. It is not difficult to show that the method can take $O(N^n)$ operations, where n is the degree of $P(W,z)$ with respect to W. Hence the classical method is very slow when n is large.

The main result of this paper is that every algebraic function can be computed fast. Let $M(N)$ denote the number of operations sufficient to multiply two Nth degree polynomials over the field Δ. Let $C(N)$ be the number of operations needed to compute any algebraic function. We prove that

$$C(N) = O(nM(N)).$$

Since $M(N) = O(N^2)$ (or $M(N) = O(N \log N)$ if the FFT is used), our algorithms are considerably faster than the classical method even for moderate n. It is an open problem whether or not a general algebraic function can be computed in less than $O(M(N))$ operations.

The "fast computation" of the title is because the coefficients of a "regular" problem can always be computed fast by iteration (Section 5) and the general problem can be reduced to a regular problem (Section 6) with cost independent of N.

Brent and Kung [1976] showed that the cost for reversion of a polynomial, which is a very special case of an algebraic function (see discussion later in this section), is $O((N \log N)^{\frac{1}{2}} M(N))$. We stated above that the cost of expanding an algebraic function is $O(nM(N))$. These results are reconciled by the observation that we are considering the case that the degree n of $P(W,z)$ with respect to W is fixed and independent of N, while Brent and Kung considered the case where $n = N$.

There are known examples of fast computation using Newton-like iteration in settings such as algebraic number theory (Bachman [1964]), power series computation (Kung [1974], Brent and Kung [1976]), and the Zassenhaus construction in p-adic analysis (Yun [1976]). Fast computation of algebraic functions raises certain issues not present in these other settings; see especially Section 6. As we will see in Section 5, there is nothing special about Newton-like iteration; any "normal iteration" can be used.

Although the complexity results are stated asymptotically, Theorems 5.1 and 6.1 give non-asymptotic analyses of the algorithms. Hence various non-asymptotic analyses can also be carried out.

We are interested in the computation of algebraic functions for a number of reasons. These include

1. A number of problems where fast algorithms are known are special cases of algebraic functions. (More details are given below.)

2. There are numerous applications. For example, many generating functions of combinatorial analysis and functions arising in mathematical physics are algebraic functions. The integrands of elliptic and more generally Abelian integrals are algebraic functions. See Section 9 for an example.

3. Algorithms for expanding algebraic functions are needed in systems for symbolic mathematics such as MACSYMA (Moses [1974]).

4. Algebraic functions are of theoretical interest in many areas of mathematics. These include integration in finite terms (Ritt [1948]), theory of plane curves (Walker [1950]), elliptic function theory (Briot and Bouquet [1859]), complex analysis (Ahlfors [1966], Saks and Zygmund [1971]), and algebraic geometry (Lefschetz [1953]). Algebraic function theory is a major subject in its own right. See, for example, Bliss [1933] and Eichler [1966].

We exhibit special cases of algebraic functions where fast algorithms are known.

A. Reciprocal of a polynomial:

$$P(W,z) = A_1(z)W - 1.$$ (See Kung [1974].)

(Actually Kung uses $P(W,z) = W^{-1} - A_1(z)$ which is not of the form (1.1), and allows $A_1(z)$ to be a power series.)

B. nth root of a polynomial:

$P(W,z) = W^n - A_0(z)$. (See Brent [1976, Section 13] where the $A_0(z)$ is allowed to be a power series.)

C. Reversion of a polynomial:

Let f be a given polynomial with zero constant term. We seek a function g such that $f(g(z)) = z$. To see this is a special case of an algebraic function, let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x$. Then we seek $g(x)$ such that $a_n g^n(z) + \ldots + a_1 g(z) - z = 0$. This is an instance of our general problem with $A_i(z) = a_i$, $i=1,\ldots,n$, $A_0(z) = -z$.

See Brent and Kung [1976].

We summarize the results of this paper. In Section 2 we show that without loss of generality we can take $z_0 = 0$ and assume $A_n(0) \neq 0$. Notation is established and a few basic facts from algebraic function theory are summarized in Section 3. The concept of normal iteration is introduced in Section 4 and convergence of normal iterations for regular problems is established in Section 5. In Section 6 we state and analyze the Newton Polygon Process, which reduces the general problem to a regular problem. A symbolic mode of computation with exact arithmetic is introduced in Section 7. Section 8 shows that $C(N) = O(nM(N))$. In Section 9 we give a number of examples, several of which are more general than the theory of the preceding sections. The final section discusses extensions of the work presented here.

In this paper we analyze algorithms under the assumption that the coefficient of power series are "non-growing", e.g., all coefficient computations are done in a finite field or in finite-precision floating-point arithmetic. An analysis dealing with variable-precision coefficients is yet to be performed.

2. PRELIMINARY TRANSFORMATIONS

Recall that we wish to compute one of the expansions around z_0 of the algebraic function $S(z)$ corresponding to

$$P(W,z) = A_n(z)W^n + \ldots + A_0(z),$$

i.e., $P(S(z),z) \equiv 0$. In this section we show that after two simple transformations we need only deal with the case that $z_0 = 0$ and $A_n(0) \neq 0$. If we transform $P(W,z)$ to $\bar{P}(W,z)$, then $\bar{S}(z)$ is defined by $\bar{P}(\bar{S}(z),z) \equiv 0$.

Consider first the case $z_0 = \infty$. Let

$$\bar{P}(W,z) = z^m P(W,\frac{1}{z}) \tag{2.1}$$

where $m = \max_{0 \leq i \leq n} (\deg A_i)$. By definition, an expansion of $S(z)$ around $z_0 = \infty$ is an expansion of $\bar{S}(z)$ around $z_0 = 0$.

Consider next the case that z_0 is any finite complex number. Define

$$\bar{P}(W,z) = P(W,z+z_0).$$

An expansion of $\bar{S}(z)$ around the origin is an expansion of $S(z)$ around $z = z_0$.

For the remainder of this paper we shall therefore take $z_0 = 0$.

Let $A_n(0) = 0$. Then the algebraic function $S(z)$ corresponding to $P(W,z)$ has one or more expansions with negative powers. Using the following transformation, we need only deal with expansions with non-negative powers. It is convenient to use ord notation.

Definition 2.1. Let $A(z)$ be an integral or fractional power series. If $A(z) \not\equiv 0$, then ord(A) denotes the degree of the lowest degree term in $A(z)$. If $A(z) \equiv 0$, then $\text{ord}(A) = \infty$.

Choose non-negative integers μ and λ to satisfy the following conditions:

$$\mu + \mathrm{ord}(A_n) = n\lambda,$$

$$\mu + \mathrm{ord}(A_i) \geq i\lambda, \quad i=1,\ldots,n-1.$$

Let

$$\bar{P}(W,z) = z^{\mu}P(W/z^{\lambda},z).$$

Then the coefficients of $\bar{P}(W,z)$, $\bar{A}_i(z)$, are polynomials with $\bar{A}_n(0) \neq 0$, and $\bar{S}(z)$ has only expansions with non-negative powers. Since the expansions of $S(z)$ are those of $\bar{S}(z)$ divided by z^{λ}, it suffices to compute expansions of $\bar{S}(z)$. For the remainder of this paper, we therefore assume that $A_n(0) \neq 0$. (One should note, however, that the results of Section 5 hold without the assumption.)

3. FACTS FROM ALGEBRAIC FUNCTION THEORY

We introduce some notation and state a basic result of algebraic function theory which characterizes the expansions of the algebraic function corresponding to

$$P(W,z) = A_n(z)W^n + \ldots + A_0(z).$$

There exist r positive integers $d_1,\ldots,d_r$ such that $d_1 + \ldots + d_r = n$ and the expansions of the algebraic function are given by

$$S_{i,j}(z) = \sum_{\ell=0}^{\infty} s_{i,\ell}\, \xi_i^{j\ell} \cdot z^{\frac{\ell}{d_i}}. \tag{3.1}$$

for $i=1,\ldots,r$ and $j=0,\ldots,d_i-1$, where ξ_i is a primitive d_ith root of unity and the $s_{i,\ell}$ are complex numbers. For each i, the expansions $S_{i,j}$, $j=0,\ldots,d_i-1$, are said to constitute a cycle.

The problem considered in this paper is to compute one expansion of an algebraic function. For notational convenience, let the expansion be denoted by

$$S(z) = \sum_{\ell=0}^{\infty} s_\ell \cdot z^{\frac{\ell}{d}}.$$

Hence our problem can be formulated as that of computing the value of d and the coefficients $s_0, s_1, \ldots$. (In this paper S(z) represents either an algebraic function or one of its expansions, depending upon the context.) Note that since

$$P(S(z),z) \equiv 0,$$

we have

$$P(s_0,0) = 0.$$

Thus, s_0 is a zero of the numerical polynomial $P(W,0)$. We say our problem is <u>regular</u> with respect to s_0 if s_0 is a simple zero of $P(W,0)$. (In this definition, we allow $A_n(0)$ to be 0 .) For a regular problem, we have $d = 1$, that is, the expansion $S(z)$ is an integral power series. In Section 5, we shall show that a regular problem can always be solved by iteration. In Section 6, we shall show how the general problem can be transformed to a regular problem.

4. NORMAL ITERATIONS

We introduce the concept of a normal numerical iteration. We give a novel definition of the order of a normal iteration which is convenient for the application to power series iteration. In the following section we will show that a normal iteration with order greater than unity will always converge if used for a regular problem.

Let $p(w)$ be the numerical polynomial $P(W,0)$, let s be a zero of $p(w)$, and let $e^{(i)} = w^{(i)} - s$ denote the error of the ith iterate. To motivate the definition of normal iteration we first consider two examples.

Example 4.1. Newton Iteration

$$w^{(i+1)} = w^{(i)} - \frac{p(w^{(i)})}{p'(w^{(i)})} .$$

From the Taylor series expansions

$$p(w^{(i)}) = p'(s)e^{(i)} + \frac{p''(s)}{2} (e^{(i)})^2 + \ldots ,$$

and

$$p'(w^{(i)}) = p'(s) + p''(s)\ e^{(i)} + \ldots,$$

we have

$$(4.1) \quad e^{(i+1)} = \frac{p''(s)}{2p'(s)}(e^{(i)})^2 + \sum_{j=3}^{\infty} c_j \cdot (e^{(i)})^j$$

where the c_j are rational expressions of the derivatives of p at s, with powers of $p'(s)$ as the denominators. ■

Example 4.2. Secant Iteration

$$w^{(i+1)} = w^{(i)} - \frac{w^{(i)}-w^{(i-1)}}{p(w^{(i)})-p(w^{(i-1)})} \cdot p(w^{(i)}).$$

Using the Taylor series expansions of $p(w^{(i)})$ and $p(w^{(i-1)})$, we obtain

$$(4.2)\quad e^{(i+1)} = \frac{p''(s)}{2p'(s)}\, e^{(i)}e^{(i-1)} + \sum_{\substack{j+\ell\geq 3\\ j,\,\ell\geq 1}} c_{j\ell} \cdot (e^{(i)})^{j}(e^{(i-1)})^{\ell},$$

where the $c_{j\ell}$ are rational expressions of the derivatives of p at s, with powers of p'(s) as the denominators. ■

Consider now a general iteration

$$(4.3)\quad w^{(i+1)} = \psi(w^{(i)}, w^{(i-1)}, \ldots, w^{(i-m)}),$$

which is defined in terms of rational expressions of p and its derivatives.

Assume that by using Taylor series expansions, we can derive

$$(4.4)\quad e^{(i+1)} = \sum_{j_i\geq 0} c_{j_0,\ldots,j_m} \cdot (e^{(i)})^{j_0} \ldots (e^{(i-m)})^{j_m}$$

where the $c_{j_0,\ldots,j_m}$ are rational expressions of the derivatives of p at s.

Definition 4.1. ψ is said to be a normal iteration if the denominator of each $c_{j_0,\ldots,j_m}$ is a power of p'(s). ■

From (4.1) and (4.2) we have that both Newton iteration and secant iteration are normal. In fact, most commonly used iterations are normal. We prove that the classical one-point inverse interpolatory iterations ψ_ρ (see Traub [1964, Section 5.1]; in particular, ψ_2 is the Newton iteration) are normal. Let q denote the inverse function to p and $v^{(i)} = p(w^{(i)})$. Then

$$s = q(0) = q(v^{(i)}) - q'(v^{(i)})v^{(i)} + \frac{1}{2}\, q''(v^{(i)})(v^{(i)})^2 + \ldots .$$

By definition of ψ_ρ,

$$s = \psi_\rho(w^{(i)}) + \sum_{j \geq \rho} \frac{(-1)^j}{j!} q^{(j)}(v^{(i)})(p(w^{(i)}))^j,$$

and

$$e^{(i+1)} = \sum_{j \geq \rho} \frac{(-1)^{j+1}}{j!} q^{(j)}(v^{(i)})(p(w^{(i)}))^j.$$

Note that

$$p(w^{(i)}) = p'(s)e^{(i)} + \frac{1}{2} p''(s)(e^{(i)})^2 + \ldots$$

and that $q^{(j)}(v^{(i)})$ is a rational expression of $p^{(k)}(w^{(i)})$ for $k=1,\ldots,j$ and has the denominator $(p'(w^{(i)}))^j$. Expanding the $p^{(k)}(w^{(i)})$ around s shows that ψ_ρ is a normal iteration.

Definition 4.2. For a normal iteration ψ defined by (4.3) and satisfying (4.4), we define the order ρ of ψ by

$$\rho = \sup\{r \mid r^{m+1} \leq j_0 r^m + j_1 r^{m-1} + \ldots + j_m \text{ for all } (j_0,\ldots,j_m)$$
$$\text{such that } c_{j_0,\ldots,j_m} \neq 0 \text{ for some polynomial } p.\} \quad \blacksquare$$

By (4.1), it is easy to check that the Newton iteration has order 2. In general, it can be shown that the one-point inverse interpolatory iteration ψ_ρ has order ρ. Consider now the secant iteration. By (4.2), the order of the iteration is given by

$$\rho = \sup\{r \mid r^2 \leq jr + \ell \text{ for all } j, \ell \geq 1\},$$

which is equivalent to $\rho = \sup\{r \mid r^2 \leq r + 1\}$. Hence ρ is the positive root of $r^2 = r+1$, i.e., $\rho = \phi = (1+\sqrt{5})/2$.

5. REGULAR PROBLEMS: NORMAL ITERATIONS ON POWER SERIES

We show how normal numerical iterations with order greater than unity can always compute an expansion of an algebraic function for a regular problem. The main result is Theorem 5.1. As a corollary of this theorem we show that a Newton-like iteration always "converges quadratically". We also show the convergence of a secant-like iteration. We end the section with an example of a convergent first order iteration.

We begin with some definitions. Recall that a meromorphic series is a power series with a finite number of negative powers.

Definition 5.1. Given a meromorphic series $A(z)$ and a real number σ, then by the notation

$$B(z) \equiv A(z) \pmod{z^{\sigma}}$$

we mean $B(z)$ is a finite series consisting of all terms of $A(z)$ of degree $< \sigma$. ■

Let Ψ be a normal numerical iteration. Let the numbers $w^{(i)},\ldots,w^{(i-m)}$ in (4.3), the defining relation for Ψ, be replaced by meromorphic series $W^{(i)}(z),\ldots,W^{(i-m)}(z)$. Then the iterate $W^{(i+1)}(z)$ defined by

$$W^{(i+1)}(z) = \Psi(W^{(i)}(z),\ldots,W^{(i-m)}(z))$$

is in general a meromorphic series, provided that it is well-defined. Let $E^{(i)}(z) = W^{(i)}(z) - S(z)$ denote the error of the ith iterate.

Definition 5.2. We say an iteration on meromorphic series converges if

$$\lim_{i\to\infty} \operatorname{ord}(E^{(i)}) = \infty.$$

Our main result for regular problems is given by the following theorem.

Theorem 5.1. If

(i) $P(s_0,0) = 0$, $P'(s_0,0) \neq 0$,

(ii) ψ is a normal iteration with order $\rho > 1$,

(iii) $W^{(0)}(z) = s_0$, $W^{(1)}(z),\ldots,W^{(m)}(z)$ are polynomials in z such that $\operatorname{ord}(E^{(i)}) \geq \rho^i$ for $i=0,\ldots,m$, where $S(z)$ is the expansion starting with the term s_0,

(iv) $\psi(W^{(i)}(z),W^{(i-1)}(z),\ldots,W^{(i-m)}(z))$, $i=m,m+1,\ldots$, is a well-defined meromorphic series,

then the iterates

$$W^{(i+1)}(z) \equiv \psi(W^{(i)}(z),W^{(i-1)}(z),\ldots,W^{(i-m)}(z)) \pmod{z^{\rho^{i+1}}}$$

satisfy the property that

$$\operatorname{ord}(E^{(i+1)}) \geq \rho^{i+1}, \tag{5.1}$$

and hence the iteration converges.

Proof. Let $i = m$. By (iv), $\psi(W^{(m)}(z),W^{(m-1)}(z),\ldots,W^{(0)}(z))$ is a well-defined meromorphic series. Since (4.4) is derived by Taylor series expansions and since the Taylor series expansion is valid over meromorphic series, we have that

$$E^{(m+1)}(z) = \sum_{j_i\geq 0} C_{j_0,\ldots,j_m}(E^{(m)}(z))^{j_0}\ldots(E^{(0)}(z))^{j_m} \tag{5.2}$$

holds for meromorphic series. The constant term of $P'(S(z),z)$ is $P'(s_0,0)$, which is non-zero by condition (i). Thus by conditions (ii) and (iii), (5.2) implies that

$$\text{ord}(E^{(m+1)}) \geq \min(j_0\rho^m + j_1\rho^{m-1} + \ldots + j_m)$$

where the minimum is taken over all the $(j_0,\ldots,j_m)$ such that $C_{j_0,\ldots,j_m}$ is non-zero for some $P(W,z)$. By the definition of ρ in Section 4, we have

$$\text{ord}(E^{(m+1)}) \geq \rho^{m+1}.$$

By induction, (5.1) can be established for $i=m+1,m+2,\ldots$, using similar arguments. The convergence of the iteration follows immediately from Definition 5.2. ■

Remark 5.1. Thus well-defined normal iterations on regular problems always converge. This behavior is strikingly different from the behavior of these iterations on numerical polynomials where only local convergence is assured unless strong conditions are imposed. Note that the expansion $S(z)$ may converge in only a small disk around the origin; we shall not pursue the domain of convergence here. ■

Remark 5.2. (5.1) shows that $W^{(i)}$ is a power series with non-negative powers only rather than a meromorphic series. Until this fact was established it was necessary to work over the field of meromorphic series. ■

Remark 5.3. Observe that we do not define order for power series valued iteration but only for normal numerical iterations. ■

Remark 5.4. Note that in Theorem 5.1 we need not assume that $A_n(0) \neq 0$. This fact will be used in the proof of Theorem 6.1. ■

We apply Theorem 5.1 to two specific iterations. We begin with a Newton-like iteration, which is defined by (5.3) below. This iteration is obtained from the numerical Newton iteration. In the power series setting we hesitate to call it Newton iteration, since Newton [1670] actually used a different method for computing the expansion. His method computes one coefficient per iteration and in general is not as efficient as the Newton-like iteration defined below. We will discuss the Newton-like iteration in some detail since we anticipate it will be one of the most commonly used iterations in practice. Here and elsewhere we use the notation $P'(W,z) \equiv \frac{\partial P}{\partial W}(W,z)$. Recall that the numerical Newton iteration is a normal iteration of order 2. From Theorem 5.1 we have

Corollary 5.1.* If

(i) $P(s_0,0) = 0$ and $P'(s_0,0) \neq 0$,

(ii) $W^{(0)} = s_0$, i.e., $\operatorname{ord}(E^{(0)}) \geq 1$,

then the iterates $W^{(i)}$ generated by the Newton-like iteration,

$$(5.3)\quad W^{(i+1)}(z) \equiv W^{(i)}(z) - \frac{P(W^{(i)}(z),z)}{P'(W^{(i)}(z),z)} \pmod{z^{2^{i+1}}}$$

are well-defined and satisfy

$$(5.4)\quad \operatorname{ord}(E^{(i)}) \geq 2^i$$

for i=0,1,2,..., and hence the iteration converges.

*A result similar to Corollary 5.1 has been proven independently by Professor J. Lipson (Private Communication).

Proof. We need only show that the iterations $W^{(i)}(z)$ are all well-defined. This holds since for all i the constant term in $P'(W^{(i)},z)$ is $P'(s_0,0)$, which is non-zero, ■

Remark 5.5. If we define the valuation of a power series $A(z)$ to be $b^{-\mathrm{ord}(A)}$ where b is any positive constant, then Corollary 5.1 follows from a known theorem in valuation theory (see Bachman [1964, Ch. II, Theorem 4.2]).

It is easy to show that if $S(z)$ is a polynomial of degree q, then iteration (5.3) will compute it in $\lfloor \log_2 q \rfloor + 1$ iterations. By a slight modification of the hypotheses of Corollary 5.1 we can replace the inequality (5.4) by equality.

Corollary 5.2. If

(i) $P(s_0,0) = 0$, $P'(s_0,0) \neq 0$, $P''(s_0,0) \neq 0$,

(ii) $W^{(0)} = s_0$, $\mathrm{ord}\ E^{(0)} = 1$,

then the iterates generated by the Newton-like iteration satisfy $\mathrm{ord}(E^{(i)}) = 2^i$. ■

Corollaries 5.1 and 5.2 can easily be generalized to any one-point inverse interpolatory iteration Ψ_0.

As our second example we consider a secant-like iteration. One has to be somewhat careful in defining this iteration. A straightforward approach would generate iterates by

$$(5.5)\quad W^{(i+1)} \equiv W^{(i)} - \frac{W^{(i)}-W^{(i-1)}}{P(W^{(i)})-P(W^{(i-1)})} \cdot P(W^{(i)}) \pmod{z^{\phi^{i+1}}}$$

where $\phi = (1+\sqrt{5})/2$. Then $W^{(i+1)}$ becomes undefined when $W^{(i)} = W^{(i-1)}$. This happens when there is a "large" gap between the degrees of two consecutive terms, in the expansion which we want to compute. A solution to the problem is given in the following Corollary. The idea is to use a perturbed $W^{(i)}$ in

(5.5) so that the denominator is guaranteed to be non-zero.

Corollary 5.3. If

$$\text{(i)} \quad P(s_0,0) = 0,\ P'(s_0,0) \neq 0,$$
$$\text{(ii)} \quad W^{(0)} = s_0,\ W^{(1)} = s_0 + s_1 z,$$

then the iterates $W^{(i)}$ generated by

$$(5.6) \quad W^{(i+1)} \equiv \bar{W}^{(i)} - \frac{\bar{W}^{(i)} - W^{(i-1)}}{P(\bar{W}^{(i)}) - P(W^{(i-1)})} \cdot P(\bar{W}^{(i)}) \pmod{z^{F_{i+3}}}$$

are well-defined and satisfy

$$\operatorname{ord}(E^{(i)}) \geq F_{i+2},$$

where the F_i is the ith Fibonacci number (i.e., $F_0 = 0, F_1 = 1$ and $F_{i+1} = F_i + F_{i-1}$) and $\bar{W}^{(i)} = W^{(i)} + z^{F_{i+2}}$.

Proof. Consider the case i = 1. Clearly, $\bar{W}^{(1)} = W^{(1)} + z^2 \neq W^{(0)}$ and $\operatorname{ord}(\bar{W}^{(1)} - W^{(0)}) \leq F_3$. Since by the Taylor series expansion,

$$P(\bar{W}^{(1)}) - P(W^{(0)}) = P'(W^{(0)}) \cdot (\bar{W}^{(1)} - W^{(0)}) + \ldots,$$

and since $P'(W^{(0)})$ has a non-zero constant term $P'(s_0,0)$, we have

$$\operatorname{ord}(P(\bar{W}^{(1)}) - P(W^{(0)})) = \operatorname{ord}(\bar{W}^{(1)} - W^{(0)}) \leq F_3.$$

Hence $P(\bar{W}^{(1)}) \neq P(W^{(0)})$. This ensures that $W^{(2)}$ is well-defined by (5.6). Note that for i = 1 (4.2) holds with $E^{(1)}$ replaced by $\bar{E}^{(1)} = \bar{W}^{(1)} - S$. Thus,

$$\text{ord}(E^{(2)}) \geq \text{ord}(\bar{E}^{(1)}E^{(0)}) = \text{ord}(\bar{E}^{(1)}) + \text{ord}(E^{(0)})$$
$$\geq \min(\text{ord}(E^{(1)}), F_3) + \text{ord}(E^{(0)}) \geq F_3 + F_2 = F_4.$$

By induction, one can similarly prove that for $i=2,3,\ldots$, $W^{(i)}$ is well-defined and $\text{ord}(E^{(i)}) \geq F_{i+2}$. ■

Results similar to Corollary 5.3 hold for other suitably modified iterations with memory, (i.e., iterations with $m > 0$ in (4.3)).

So far we have only dealt with iterations of order > 1. We now consider an iteration with order one. Define

$$w^{(i+1)} = w^{(i)} - \frac{p(w^{(i)})}{p'(w^{(0)})}$$

for $i=0,1,2,\ldots$. Then

$$(5.7)\quad e^{(i+1)} = e^{(i)} - \frac{p'(s)e^{(i)} + \frac{1}{2}p''(s)e^{(i)^2} + \ldots}{p'(s) + p''(s)e^{(0)} + \ldots}$$

$$= \frac{p''(s)}{p'(s)} e^{(0)}e^{(i)} - \frac{p''(s)}{2p'(s)} (e^{(i)})^2 + \sum_{\substack{j+\ell\geq 3 \\ j\geq 0,\ \ell\geq 1}} c_{j,\ell}(e^{(0)})^j(e^{(i)})^\ell$$

where the $c_{j,\ell}$ are rational expressions whose denominators are powers of $p'(s)$. This implies that the iteration is normal and has order $\rho = 1$. We may use the iteration on power series and obtain the following theorem which is an easy consequence of (5.7):

Theorem 5.2. If

(i) $P(s_0,0) = 0$, $P'(s_0,0) \neq 0$.

(ii) $W^{(0)} = s_0$,

then the iterates $W^{(i)}$ generated by

$$W^{(i+1)}(z) \equiv W^{(i)}(z) - \frac{P(W^{(i)}(z))}{P'(W^{(0)}(z))} \pmod{z^{i+2}} \tag{5.8}$$

are well-defined and satisfy

$$\operatorname{ord}(E^{(i)}) \geq i+1,$$

and hence the iteration converges. ■

The iteration (5.8) can be used, for example, to find the initial iterates of an iteration with memory.

6. THE GENERAL PROBLEM: NEWTON POLYGON PROCESS

Recall that our general problem is to compute the value of d and the coefficients $s_0, s_1, \ldots$ of an expansion

$$S(z) = \sum_{\ell=0}^{\infty} s_\ell \cdot z^{\frac{\ell}{d}}$$

of the algebraic function corresponding to a given

$$P(W,z) = A_n(z)W^n + \ldots + A_0(z).$$

In this section, we show that the general problem can be reduced to a regular problem by transforming $P(W,z)$ to some $\bar{P}(W,z)$. The regular problem can then be solved by normal iterations, as described in Section 5.

Since $P(s_0,0) = 0$, s_0 can be obtained by finding a zero of the numerical polynomial $P(W,0)$. In this section we assume that finding a zero of a numerical polynomial is a primitive operation.* (This assumption will be removed in the next section by carrying the zeros symbolically.) If $P'(s_0,0) \neq 0$, we have a regular problem solvable by a normal iteration. Hence we assume that $P'(s_0,0) = 0$. Then s_0 is a multiple zero of the numerical polynomial $P(W,0)$ and there is more than one expansion of the algebraic function starting with s_0. We would not expect an iteration starting with $W^{(0)} = s_0$ to converge since the iteration would not "know" to which expansion it should converge. Intuitively the convergence of an iteration requires that it start with an initial segment of a unique expansion. This suggests that we find an initial segment of a unique expansion starting with s_0. The existence of the segment is guaranteed only if no two expansions coincide, i.e., the

*I.e., zeros of a polynomial can be computed to any prespecified precision.

discriminant $D(z)$ of $P(W,z)$ with respect to W is not identically equal to zero. Therefore, in this section we shall assume that

$$D(z) \not\equiv 0.$$

The assumption holds when $P(W,z)$ is irreducible or simply when $P(W,z)$ is square-free (Walker [1950, Theorem 3.5]). Hence we can make this condition hold by using factorization or square-free decomposition algorithms but do not pursue this here.

A classical method for finding an initial segment of a unique expansion uses a geometric aide known as the Newton Polygon, which provides a convenient tool for analyzing a set of inequalities. (Some authors refer to Puiseux's Theorem because of the work of Puiseux [1850] but clearly the idea originated with Newton [1670, p. 50].) The method has not been subject to algorithmic analysis.

We state the Newton Polygon Process adapting, with some modifications, the description in Walker [1950]. In Theorem 6.1 we show that the Newton Polygon Process transforms the general problem to a regular problem. Theorem 6.1 also gives the connection between the number of identical terms in at least two expansions and the number of Newton Polygon stages. Theorem 6.2 gives an a priori bound on the number of stages which differs by at most a factor of two from the optimal bound. Example 6.1 shows that in general $P(W,z)$ must be transformed to a new polynomial $\bar{P}(W,z)$; it is not enough to compute an initial segment of a unique expansion and use it as the initial iterate for a normal iteration on the original polynomial $P(W,z)$.

In the following algorithm, let $A_{i,k}(z)$ be the coefficient of W^i in $P_k(W,z)$. If $A_{i,k}(z) \not\equiv 0$, let $a_{i,k}z^{\alpha_{i,k}}$ be the lowest degree term in $A_{i,k}(z)$.

Newton Polygon Process

N1. $k \leftarrow 1$, $P_k(W,z) \leftarrow P(W,z)$.

N2. Plot the points $f_{i,k} = (i,\alpha_{i,k})$ on the xy plane for i such that $A_{i,k}(z) \not\equiv 0$. Join $f_{0,k}$ to $f_{n,k}$ with a convex polygon arc each of whose vertices is an $f_{i,k}$ and such that no $f_{i,k}$ lies below any line extending an arc segment.

N3. If $k = 1$, choose any segment $y + \gamma_k x = \beta_k$ of the arc. If $k > 1$, choose a segment with $\gamma_k > 0$. (Such a segment always exists.) Let g_k denote the set of indices i for which $f_{i,k}$ lies on the chosen segment. Solve the polynomial equation

$$\sum_{i \in g_k} a_{i,k} x^i = 0. \tag{6.1}$$

Let c_k be any of the non-zero roots. (Such a non-zero solution always exists.)

N4. If c_k is a simple zero, go to N6; else go to N5.

N5. $P_{k+1}(W,z) \leftarrow z^{-\beta_k} \cdot P_k(z^{\gamma_k}(W+c_k),z)$, $k \leftarrow k+1$. Go to N2.

N6. $t \leftarrow k$. (Hence t represents the number of stages taken by the Newton Polygon Process.)

$$\hat{P}(W,z) \leftarrow z^{-\beta_t} \cdot P_t(z^{\gamma_t}W,z),$$

$$\bar{P}(W,z) \leftarrow \hat{P}(W,z^d),$$

where d is the smallest common denominator of $\gamma_1,\ldots,\gamma_t$. (γ_1 may be zero. If $\gamma_1 = 0$ we assume that γ_1 has one as its denominator.) Terminate the process. ■

Lemma 6.1. After the Newton Polygon Process terminates, the following properties hold:

(i) The coefficients of $\bar{P}(W,z)$ are polynomials in z.

(ii) c_t is a simple zero of the numerical polynomial $\bar{P}(W,0)$.

Proof. It is easy to verify (i). To prove (ii) we show that

$$\bar{P}(W,0) = \sum_{i \in g_t} a_{i,t} W^i.$$

For notational convenience, let $\alpha_{i,t} \equiv \alpha_i$, $a_{i,t} \equiv a_i$, $\beta_t \equiv \beta$, $\gamma_t \equiv \gamma$, $g_t \equiv g$ and let $\bar{g}$ denote the set complementary to g with respect to $\{0,1,\ldots,n\}$. Let

$$P_t(W,z) = (a_n z^{\alpha_n} + Q_n(z))W^n + \ldots + (a_0 z^{\alpha_0} + Q_0(z)),$$

where $\mathrm{ord}(Q_i) > \gamma_i$. Then

$$\hat{P}(W,z) = \sum_{i \in g} a_i W^i + \sum_{j \in \bar{g}} a_j z^{\alpha_j + j\gamma - \beta} W^j + \sum_{i=0}^{n} z^{i\gamma - \beta} Q_i(z) W^i.$$

Since $\beta = \alpha_i + i\gamma < \alpha_j + j\gamma$, $\forall i \in g$, $\forall j \in \bar{g}$,

$$\bar{P}(W,0) = \hat{P}(W,0) = \sum_{i \in g} a_i W^i.$$

■

Theorem 6.1. After the Newton Polygon Process terminates, the following properties hold:

(i) The general problem of computing an expansion S(z) of the algebraic function corresponding to P(W,z) has been reduced to the following regular problem: Compute the expansion $\bar{S}(z)$ starting from c_t

for the algebraic function corresponding to $\bar{P}(W,z)$. Then let

$$S(z) = \sum_{i=1}^{t-1} c_i z^{\gamma_1+\ldots\gamma_i} + z^{\gamma_1+\ldots\gamma_t} \cdot \bar{S}(z^{\frac{1}{d}}).$$

(ii) $S(z)$ is the unique expansion with starting segment $\sum_{i=1}^{t} c_i z^{\gamma_1+\ldots+\gamma_i}$,

(iii) There is more than one expansion which starts with $\sum_{i=1}^{j} c_i z^{\gamma_1+\ldots+\gamma_i}$ for every $j < t$. That is, there are at least two expansions which coincide in their first t-1 terms.

Proof. By Lemma 6.1, we conclude that the problem of computing $\bar{S}(z)$ is regular. (Note that the leading coefficient of $\bar{P}(W,z)$ may vanish at $z = 0$. See Remark 5.4.) (i) follows from $\bar{P}(W,z) = \hat{P}(W,z^d)$ and

$$\hat{P}(W,z) = z^{-(\beta_1+\ldots+\beta_t)} P\left(\sum_{i=1}^{t-1} c_i z^{\gamma_1+\ldots+\gamma_i} + z^{\gamma_1+\ldots+\gamma_t} W, z\right).$$

(ii) and (iii) hold since the Newton Polygon Process does not terminate until c_t is a simple zero. ■

Since there is only one expansion which starts with $\sum_{i=1}^{t} c_i z^{\gamma_1+\ldots+\gamma_i}$, we might expect that if this segment is taken as the initial iterate for a normal iteration then the iteration on the original polynomial $P(W,z)$

rather than on the transformed polynomial $\bar{P}(W,z)$ will converge. The following example shows this not to be the case; in general we must use the transformed problem.

Example 6.1. This problem appears in Jung [1923, p. 29] although it is not used to illustrate the point we wish to make here. Let

$$P(W,z) = W^2 - (2+z+z^3)W + 1 + z + \frac{1}{4}z^2 + z^4.$$

The two expansions are

$$S_1(z) = 1 + \frac{1}{2}z + z^{3/2} + \ldots, \quad S_2(z) = 1 + \frac{1}{2}z - z^{3/2} + \ldots .$$

Suppose that we want to compute $S_1(z)$ by the Newton-like iteration. If we take $W^{(0)} = 1 + \frac{1}{2}z + z^{3/2}$ in

$$W^{(i+1)} = W^{(i)} - \frac{P(W^{(i)},z)}{P'(W^{(i)},z)},$$

we find $W^{(1)} = 1 + \frac{1}{2}z - \frac{1}{4}z^{5/2} + \ldots$. $W^{(1)}$ differs from S_1 even in the coefficient of $z^{3/2}$! Though there is only one expansion starting with $W^{(0)}$, namely, S_1, the Newton-like iteration starting from $W^{(0)}$ does not converge to S_1. ■

We illustrate the Newton Polygon transformation, the transformations of Section 2 and the iterative process with another problem in Jung [1923, p. 31].

Example 6.2. Find all the expansions of the algebraic function corresponding to $P(W,z) = -W^3 + zW + z^2$ around $z_0 = \infty$. The first transformation of Section 2 converts $P(W,z)$ to $-z^2W^3 + zW + 1$, which is then converted by another transformation to $-W^3 + zW + z$. The Newton Polygon Process yields

$\alpha_1 = 1$, $\beta_1 = 1$, $\gamma_1 = 1/3$, $c_1 = 1$, $d = 3$ and $\bar{P}(W,z) = -W^3 + zW + 1$. Take $W^{(0)} = 1$. Then the Newton-like iteration (5.3) applied to $\bar{P}(W,z)$ gives

$$W^{(1)} = 1 + z/3, \; W^{(2)} = 1 + z/3 - z^3/81.$$

Thus

$$S(z) = z^{1/3}\bar{S}(z^{1/3}) = z^{1/3} + z^{2/3}/3 - z^{4/3}/81 + \ldots .$$

Let $T(z) = S(z)/z = z^{-2/3} + z^{-1/3}/3 - z^{1/3}/81 + \ldots$. Then an expansion of the given problem is

$$T(\tfrac{1}{z}) = z^{2/3} + \tfrac{1}{3}z^{1/3} - \tfrac{1}{81}z^{-1/3} + \ldots .$$

The other two expansions are

$$\theta z^{2/3} + \frac{\theta^2}{3} z^{1/3} - \frac{\theta}{81} z^{-1/3} + \ldots,$$

$$\theta^2 z^{2/3} + \frac{\theta}{3} z^{1/3} - \frac{\theta^2}{81} z^{-1/3} + \ldots,$$

where θ is the primitive third root of unity. ■

The following theorem gives an a priori bound on the number t of stages in the Newton Polygon Process which differs by at most a factor of two from the optimal bound.

Theorem 6.2.

(6.2) $t \leq \mathrm{ord}(D) + 1$

Furthermore for all t there exist problems for which $t = \frac{1}{2}\,\mathrm{ord}(D)$.

Proof. The theorem is trivial if $t = 1$. We assume that $t \geq 2$. Then by (iii) of Theorem 6.1, there are at least two series expansions S_1 and S_2 which agree in the first $t - 1$ non-zero terms. Write

$$S_1 = \sum_{i=1}^{\infty} s_{1,a_i} \cdot z^{\frac{a_i}{d_1}},$$

$$S_2 = \sum_{i=1}^{\infty} s_{2,b_i} \cdot z^{\frac{b_i}{d_2}},$$

where the $\{a_i\}$, $\{b_i\}$ are strictly increasing non-negative integer sequences such that none of the s_{1,a_i}, s_{2,b_i} vanish and $s_{1,a_i} = s_{2,b_i}$, $a_i/d_1 = b_i/d_2$ for i=1,...,t-1. Without loss of generality, assume $d_1 \leq d_2$. Note that the cycle which contains S_1 has the series:

$$S_{1,j} = \sum_{i=1}^{\infty} s_{1,a_i} \xi_1^{ja_i} \cdot z^{\frac{a_i}{d_1}}, \quad j=0,\ldots,d_1-1,$$

and the cycle which contains S_2 has the series:

$$S_{2,j} = \sum_{i=1}^{\infty} s_{2,b_i} \xi_2^{jb_i} \cdot z^{\frac{b_i}{d_2}}, \quad j=0,\ldots,d_2-1,$$

where $$\xi_1 = e^{\frac{2\pi\sqrt{-1}}{d_1}} \text{ and } \xi_2 = e^{\frac{2\pi\sqrt{-1}}{d_2}}.$$

Note that we do not rule out the possibility that S_1 and S_2 are in the same cycle and that therefore the cycles $\{S_{1,j}\}$ and $\{S_{2,j}\}$ are identical. Since

$$\xi_1^{ja_i} = e^{\frac{2\pi\sqrt{-1}}{d_1} ja_i}, \quad \xi_2^{jb_i} = e^{\frac{2\pi\sqrt{-1}}{d_2} jb_i}$$

and $a_i/d_1 = b_i/d_2$ for i=1,...,t-1, $S_{1,j}$ and $S_{2,j}$ agree in the first t-1 terms for j=0,...,d_1-1. Hence,

$$\operatorname{ord}(S_{1,j}-S_{2,j}) \geq \frac{b_{t-1}+1}{d_2} = \frac{a_{t-1}}{d_1} + \frac{1}{d_2} .$$

Let

$$V(z) = \prod_{j=0}^{d_1-1} (S_{1,j}(z)-S_{2,j}(z)).$$

Then

$$\begin{aligned} \operatorname{ord}(D) &\geq \operatorname{ord}(V) \\ &\geq d_1\left(\frac{a_{t-1}}{d_1} + \frac{1}{d_2}\right) \\ &\geq a_{t-1} + 1. \end{aligned}$$

Since the $\{a_i\}$ is a strictly increasing non-negative integer sequence, $a_{t-1} \geq t-2$. Thus, $\operatorname{ord}(D) \geq t-1$ which establishes (6.2). Let

$$S_1(z) = \sum_{j=0}^{t} z^j, \quad S_2(z) = S_1(z) - z^t$$

and

$$P(W,z) = (W-S_1(z))(W-S_2(z)).$$

By Theorem 6.1, the Newton Polygon Process has t stages. $\operatorname{ord}(D) = \operatorname{ord}((S_1-S_2)^2) = 2t$ which completes the proof. ■

Theorem 6.2 gives a computable a priori bound but requires the computation of ord(D). A very cheap bound is given by

Corollary 6.1.

$$t \leq m(2n-1) + 1$$

where $m = \max_{0\leq i\leq n} (\deg A_i)$.

Proof. D(z) is a determinant of order 2n-1 whose elements are polynomials of maximal degree m. Hence D(z) is a polynomial of degree at most m(2n-1). Since D(z) cannot vanish identically, $\operatorname{ord}(D) \leq m(2n-1)$. ■

7. A SYMBOLIC MODE OF COMPUTATION

The Newton Polygon Process involves computing roots of polynomial equations (6.1). Instead of actually solving the equations, in this section we carry the roots symbolically through their minimum polynomials. We assume that the underlying field Δ is one where exact arithmetic can be performed such as a finite field or the field Q of rational numbers. Then the expansions can be computed symbolically with exact arithmetic. The following example, where Δ is taken to be Q, will illustrate the idea.

Example 7.1.

$$P(W,z) = W^3 + (z+z^2)W^2 - 2z^2W - 2z^3.$$

We shall compute an expansion of the algebraic function corresponding to $P(W,z)$, using exact rational arithmetic. The first stage of the Newton Polygon Process yields $\gamma_1 = 1$, $\beta_1 = 3$ and $c_1^3 + c_1^2 - 2c_1 - 2 = 0$. Since $c_1^3 + c_1^2 - 2c_1 - 2 = (c_1^2-2)(c_1+1)$, $c_1 = \sqrt{2}$, $-\sqrt{2}$ or -1. Suppose that we are interested in the expansion starting with $\sqrt{2}$ or $-\sqrt{2}$. Instead of using an approximation to $\sqrt{2}$ or $-\sqrt{2}$, we carry c_1 symbolically through its minimal polynomial $M_1(x) = x^2 - 2$. That is,

$$c_1^2 - 2 = 0. \tag{7.1}$$

Since the equation has only simple zeros, the Newton Polygon Process terminates with $t = 1$, and

$$\begin{aligned}\bar{P}(W,z) &= z^{-3}P(zW,z)\\ &= W^3 + (1+z)W^2 - 2W - 2.\end{aligned}$$

We use the Newton-like iteration (5.3) to compute $\bar{S}(z)$ such that $\bar{P}(\bar{S}(z),z) \equiv 0$.

Let $W^{(0)}(z) = c_1$. Then

$$W^{(1)}(z) \equiv c_1 - \frac{c_1^3+(1+z)c_1^2-2c_1-2}{3c_1^2+2(1+z)c_1-2} \pmod{z^2}$$

Using (7.1), we obtain

$$W^{(1)}(z) = c_1 - \frac{1}{3}z.$$

Similarly all coefficients of z^j in $W^{(i)}(z)$ can be represented as linear polynomials in c_1 with rational coefficients. By (i1) of Theorem 6.1, a solution to the given problem is

$$S(z) = z\tilde{S}(z) = c_1 z - \frac{1}{3}z^2 + \ldots,$$

which represents both the numerical expansions starting with $\sqrt{2}z$ and $-\sqrt{2}z$. ■

In general, when the Newton Polygon Process is performed, c_k, k=1,...,t, can be carried symbolically through its minimum polynomial $M_k(x)$ over $Q(c_1,\ldots,c_{k-1})$. Then all the coefficients of the expansion S(z) are in the extension field $Q(c_1,\ldots,c_t)$. To simplify the computation, one can compute from $M_k(x)$ the minimum polynomial M(x) for c, where c is a primitive element of the extension field $Q(c_1,\ldots,c_t)$, i.e., $Q(c) = Q(c_1,\ldots,c_t)$. Then the coefficients of the expansion S(z) can all be represented by polynomials of the form $\sum_{i=0}^{h-1} q_i c^i$, where h = deg M and $q_i \in Q$. S(z) can be computed entirely with exact arithmetic. Furthermore, S(z) give a simultaneous representation of h numerical expansions; S(z) can be used to produce h numerical expansions by substituting zeros of M(x) for c in the coefficients of S(z). (This implies that $h \leq n$.)

8. ASYMPTOTIC COST ANALYSIS

In this section we analyze the cost of computing the first N terms (including zero terms) of an expansion for large N. Since the Newton Polygon Process is independent of N, by Theorem 6.1 we can without loss of generality assume the problem is regular. Furthermore, since the asymptotic results will be the same for any normal iteration with order greater than one, we shall assume that the iteration (5.3) is used. Our cost measure is the number of operations used over the field Δ. If we carry zeros symbolically as described in Section 7, then we work over an extension field $\Delta(c)$ rather than Δ. If the minimum polynomial for c is of degree h, then operations in $\Delta(c)$ are more expensive than in Δ by a factor of $O(h)$ or $O(h^2)$. Since h is independent of N, in our analysis we shall not be concerned with whether or not zeros of polynomials are carried symbolically.

Let $M(j)$ be the number of operations needed to multiply two jth degree polynomials over the field Δ. Assume that $M(j)$ satisfies the following mild condition: there are $\alpha, \beta \in (0,1)$ such that

$$(8.1) \quad M(\lceil \alpha j \rceil) \leq \beta M(\lceil j \rceil)$$

for all sufficiently large j. Observe that $W^{(i)}(z)$ is a polynomial of degree at most $2^i - 1$, and that the computing $W^{(i+1)}(z)$ by (5.3) takes $O(nM(2^i-1))$ operations. Hence the total cost of computing N terms in the expansion is $O(n(M(N) + M(\lceil N/2 \rceil) + M(\lceil N/4 \rceil) + \ldots))$, which is $O(nM(N))$ by condition (8.1). (See Brent and Kung [1976, Lemma 1.1].) We summarize the result of this section in the following

Theorem 8.1. The first N terms of an expansion of any algebraic function can be computed in O(nM(N)) operations over the field Δ.

9. EXAMPLES

We choose as our examples calculation of the Legendre polynomials through their generating function, solution of an equation with transcendental coefficients, and calculation of the expansion of a complete elliptic integral. Although the first two examples are not covered by the theory of this paper, they are covered by easy extensions of our results. Examples 9.1 and 9.3 are illustrations of the many applications of algebraic function expansions.

We use the Newton-like iteration (5.3) in all three examples with the notation:

$$P_i \equiv P(W^{(i)}(z),z),\ P'_i \equiv P'(W^{(i)}(z),z) \equiv \frac{\partial P}{\partial W^{(i)}}(W^{(i)},z^i),\ \delta_i = P_i/P'_i.$$

Within each iteration step we exhibit enough terms so that $W^{(i)}(z)$ can be computed to 2^i-1 terms.

Example 9.1. Legendre Polynomials

The generating function for Legendre polynomials,

$$(1-2tz+z^2)^{-\frac{1}{2}} = \sum_{i=0}^{\infty} L_i(t)z^i$$

satisfies

$$P(W,z,t) = (1-2tz+z^2)W^2 - 1.$$

Take $W^{(0)} = 1$. Then

$$P_0 = -2tz,\ P'_0 = 2,\ \delta_0 = -tz,\ W^{(1)} = 1+tz.$$

$$P_1 = (1-3t^2)z^2 + (2t-2t^3)z^3,\ P'_1 = 2(1-tz),\ \delta_1 = \tfrac{1}{2}(1-3t^2)z^2 + \tfrac{1}{2}(3t-5t^3)z^3,$$

$$W^{(2)} = 1 + tz + \tfrac{1}{2}(3t^2-1)z^2 + \tfrac{1}{2}(5t^3-3t)z^3.$$

Hence the first four Legendre polynomials are

$$L_0(t) = 1,\ L_1(t) = t,\ L_2(t) = \frac{1}{2}(3t^2-1) \text{ and } L_3(t) = \frac{1}{2}(5t^3-3t).$$

B. Neta, a student at CMU, computed the first 32 Legendre polynomials by this iteration using MACSYMA. ■

Example 9.2

$$P(W,z) = W^2 + (z+1)W + \sin z.$$

Note that $\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \ldots$. Take $W^{(0)} = 0$. Then

$$P_0 = z,\ P_0' = 1,\ \delta_0 = z,\ W^{(1)} = -z,$$

$$P_1 = -\frac{z^3}{6},\ P_1' = 1,\ \delta_1 = -\frac{z^3}{6},\ W^{(2)} = -z + \frac{z^3}{6}.$$ ■

Example 9.3. A Complete Elliptic Integral

Define the integral by

$$f(t) = \int_0^{\frac{\pi}{2}} (1-t^2 \sin^2 \theta)^{-1/2} d\theta.$$

Let

$$P(W,z) = (1-z)W^2 - 1,\ z = t^2 \sin^2 \theta.$$

Take $W^{(0)} = 1$. Then

$$P_0 = -z,\ P_0' = 2,\ \delta_0 = -\frac{z}{2},\ W^{(1)} = 1 + \frac{z}{2},$$

$$P_1 = -\frac{3}{4}z^2 - \frac{1}{4}z^3,\ P_1' = 2 - z,\ \delta_1 = -\frac{3}{8}z^2 - \frac{5}{16}z^3,$$

$$W^{(2)} = 1 + \frac{z}{2} + \frac{3}{8}z^2 + \frac{5}{16}z^3.$$

$W^{(2)}$ is an initial segment of the algebraic function $S(z)$ corresponding to $P(W,z)$. Since

$$f(t) = \int_0^{\frac{\pi}{2}} S(t^2 \sin^2 \theta) d\theta,$$

$$f(t) = \eta_0 + \frac{1}{2}\eta_1 t^2 + \frac{3}{8}\eta_2 t^4 + \frac{5}{16}\eta_3 t^6 + \ldots,$$

where

$$\eta_i = \int_0^{\frac{\pi}{2}} \sin^{2i}\theta d\theta.$$

For this simple example the result can be obtained directly by a binomial expansion but this cannot of course be done in general. ■

10. EXTENSIONS

Our aim in this paper has been to show that algebraic functions form an interesting and useful domain in which to do algorithmic and complexity analysis and to exhibit fast algorithms for computing any expansion of an algebraic function. In this initial paper we have restricted ourselves to the "pure" case of algebraic functions where $P(W,z)$ is a polynomial in W with polynomial coefficients. We list some additional problems which we hope to discuss in the future. For a number of these our results (especially on regular problems) apply with minor modifications; others will require major new results.

1. Let W be a scalar variable but take z to be a vector variable. Results similar to those in Section 5 should hold. We have seen this case in Example 9.1.

2. Let the coefficients of P, $A_i(z)$, be power series (rather than polynomials). Results similar to those in Section 5 should hold. See Example 9.2.

3. Let both W and z be vector variables. This is the fully multivariate case, which, except for regular problems, is in general very difficult.

4. The domain over which we have worked is not algebraically closed since problems with polynomial coefficients lead to solutions represented by fractional power series. If the coefficients are fractional power series, the domain is algebraically closed (Puiseux's Theorem, see, e.g., Lefschetz [1953]) and this is therefore a natural setting. The Newton-like iteration is still valid on fractional power series for regular problems.

5. The field Δ need not be restricted to the complex number field. It is of particular interest to extend all the results to finite fields.

6. An important computational model is the "fully symbolic" one where the coefficients of the expansion series are expressed as functions of the input coefficients.

7. Perform complexity analysis which includes the cost due to the "growth" of coefficients.

ACKNOWLEDGMENTS

We thank H. Woźniakowski, R. Fateman, B. Neta, and A. Werschulz for their comments on the manuscript.

BIBLIOGRAPHY

Ahlfors [1966] Ahlfors, Lars V., Complex Analysis, Second Edition, McGraw-Hill, New York, 1966.

Bachman [1964] Bachman, G., Introduction to P-Adic Numbers and Valuation Theory, Academic Press, New York, 1964.

Bliss [1933] Bliss, Gilbert Ames, Algebraic Functions, Amer. Math. Soc. Colloquium Publications, Volume XVI, 1933.

Brent [1976] Brent, Richard P., "Multiple-Precision Zero-Finding Methods and the Complexity of Elementary Function Evaluation," in Analytic Computational Complexity, edited by J. F. Traub, Academic Press, New York, 1976, 151-176.

Brent and Kung [1976] Brent, R. and Kung, H. T., Fast Algorithms for Manipulating Formal Power Series, Technical Report, Computer Science Department, Carnegie-Mellon University, January 1976.

Briot and Bouquet [1859] Briot, C. and Bouquet, J., Théorie des Fonctions Elliptiques, Mallet-Bachelier, Paris, 1859.

Eichler [1966] Eichler, M., Introduction to the Theory of Algebraic Numbers and Functions, translated by G. Striker, Academic Press, New York, 1966.

Jung [1923] Jung, Heinrich W. E., Einführung in die Theorie der Algebraischen Funktionen einer Veränderlichen, Walter de Gruyter, Berlin, 1923.

Kung [1974] Kung, H. T., "On Computing Reciprocals of Power Series," Numer. Math. 22, 1974, 341-348.

Lefschetz [1953] Lefschetz, S., Algebraic Geometry, Princeton University Press, Princeton, New Jersey, 1953.

Moses [1974] Moses, J., "MACSYMA - The Fifth Year," SIGSAM Bulletin 31, August 1974, 105-110.

Newton [1670] Newton, Isaac, "Methods of Series and Fluxions," in The Mathematical Papers of Isaac Newton Volume III, edited by D. T. Whiteside, Cambridge University Press, 1969.

Puiseux [1850] Puiseux, V. A.,"Recherches Sur Les Fonctions Algébriques," J. Math. 15 (1850), 365-480.

Ritt [1948] Ritt, J. F., Integration in Finite Terms, Columbia University Press, 1948.

Saks,and Zygmund [1971] Saks, S. and Zygmund, A., Analytic Functions, Third Edition, Elsevier, New York, 1971.

Traub [1964] Traub, J. F., Iterative Methods for the Solution of Equations, Prentice-Hall, Englewood Cliffs, New Jersey, 1964.

Walker [1950] Walker, Robert J., Algebraic Curves, Princeton University Press, Princeton University, 1950.

Yun [1976] Yun, David Y. Y., "Hensel Meets Newton - Algebraic Constructions in an Analytic Setting," in Analytic Computational Complexity, edited by J. F. Traub, Academic Press, New York, 1976, 205-216.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* ALL ALGEBRAIC FUNCTIONS CAN BE COMPUTED FAST		5. TYPE OF REPORT & PERIOD COVERED Interim 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) H. T. Kung and J. F. Traub		8. CONTRACT OR GRANT NUMBER(s) N00014-76-C-0370, NR 044-422
9. PERFORMING ORGANIZATION NAME AND ADDRESS Carnegie-Mellon University Computer Science Dept. Pittsburgh, PA 15213		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Office of Naval Research Arlington, VA 22217		12. REPORT DATE July 1976 13. NUMBER OF PAGES 43
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)*		15. SECURITY CLASS. *(of this report)* UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)* The expansions of algebraic functions can be computed "fast" using the Newton Polygon Process and any "normal" iteration. Let M(j) be the number of operations sufficient to multiply two jth degree polynomials. It is shown that the first N terms of an expansion of any algebraic function defined by an nth degree polynomial can be computed in $O(n(M(N))$ operations, while the classical method needs $O(N^n)$ operations. Among the numerous applications of algebraic functions are symbolic methematics and combinatorial analysis. Reversion, reciprocation, and nth root of a polynomial are all special cases of algebraic functions.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*