THE COMPUTATIONAL COMPLEXITY OF ALGEBRAIC NUMBERS*

H. T. Kung
Carnegie-Mellon University
Pittsburgh, Pa.

ABSTRACT

Let $\{x_i\}$ be a sequence approximating an algebraic number α of degree r, and let $x_{i+1} = \varphi(x_i, x_{i-1}, \ldots, x_{i-d+1})$, for some rational function φ with integral coefficients. Let M denote the number of multiplications or divisions needed to compute φ and let $\bar{M}$ denote the number of multiplications or divisions, except by constants, needed to compute φ. Define the multiplication efficiency measure of $\{x_i\}$ as $E(\{x\}) = \frac{\log_2 p}{M}$ or as $\bar{E}(\{x_i\}) = \frac{\log_2 p}{\bar{M}}$, where p is the order of convergence of $\{x_i\}$. Kung [1] showed that $\bar{E}(\{x_i\}) \le 1$ or equivalently, $\bar{M} \ge \log_2 p$. In this paper we show that (i) $\bar{M} \ge \log_2[r(\lceil p\rceil-1) + 1] - 1$; (ii) if $E(\{x_i\}) = 1$ then α is a rational number; (iii) if $\bar{E}(\{x_i\}) = 1$ then α is a rational or quadratic irrational number. This settles the question of when the multiplication efficiency $E(\{x_i\})$ or $\bar{E}(\{x_i\})$ achieves its optimal value of unity.

1. INTRODUCTION

The effort required to approximate an algebraic number should increase with its degree. In this paper we prove this assertion in a precise sense. We also show that the optimal efficiency of approximation can be achieved only for algebraic numbers which have very low degrees; in fact, degree one or degree two.

Let $\{x_i\}$ be a convergent sequence generated by $x_{i+1} = \varphi\,(x_i, x_{i-1}, \ldots, x_{i-d+1})$ for some rational function φ with integral coefficients. Let M denote the number of multiplications or divisions needed to compute φ and let $\bar{M}$ denote the number of multiplications or divisions, except by constants, needed to compute φ. Define the multiplication efficiency measure of $\{x_i\}$ as $E(\{x_i\}) = \frac{\log_2 p}{M}$ or as $\bar{E}(\{x_i\}) = \frac{\log_2 p}{\bar{M}}$, where p is the order of convergence of $\{x_i\}$. Of course, $E(\{x_i\}) \le \bar{E}(\{x_i\})$. Kung [1] showed that $\bar{E}(\{x_i\}) \le 1$, that is, $\bar{M} \ge \log_2 p$. In this paper we show that, if $\{x_i\}$ is a sequence approximating an algebraic number α of degree r, then

(i) $\bar{M} \ge \log_2[r(\lceil p\rceil-1) + 1] - 1$,

(ii) $\bar{E}(\{x_i\}) = O([\log_2 r]^{-1})$ as $r \to \infty$, provided that we only consider sequences $\{x_i\}$ of order of convergence $p \le U$, for some constant U,

(iii) if $E(\{x_i\}) = 1$ then α is a rational number,

(iv) if $\bar{E}(\{x_i\}) = 1$ then α is a rational or quadratic irrational number.

Another efficiency measure defined as $\frac{\log_2 p}{A}$

*This work was supported in part by the National Science Foundation under grant GJ-32111 and the Office of Naval Research under Contract N00014-67-A-0314-0010, NR 044-422.

where A is the number of arithmetic operations needed to compute φ has been studied by Kung and Traub [2].

2. NOTATION

We work over either the field of real numbers or the field of complex numbers. If we work over the field of real numbers, we define the integers to be the rational integers, for example, 1, -2, 3, while if we work over the field of complex numbers, we define the integers to be the Gaussian integers, for example, 1+3i, 1-i, 3-2i. Hence the word "integers" in the rest of the paper will refer to either the rational integers or the Gaussian integers depended upon whether the base field is the field of real numbers or the field of complex numbers.

Let I be the integral domain of integers and let $y_1,\ldots,y_d$ be indeterminants over I. Define $I[y_1,\ldots,y_d](I(y_1,\ldots,y_d))$ to be the ring (field) of polynomials (rational functions) in $y_1,\ldots,y_d$ with coefficients in I.

Let $\varphi(y_1,\ldots,y_d) \in I(y_1,\ldots,y_d)$. Define $M(\varphi)(\bar{M}(\varphi))$ to be the number of multiplications or divisions (respectively, except by constants) needed to compute the value of $\varphi(y_1,\ldots,y_d)$ from an arbitrary point $(y_1,\ldots,y_d)$.

For every $\varphi(y_1,\ldots,y_d) \in I(y_1,\ldots,y_d)$ define $\varphi_i(y_1,\ldots,y_d)$, i=1,2, to be those two relatively prime polynomials in $I[y_1,\ldots,y_d]$ such that

$$\varphi(y_1,\ldots,y_d) = \frac{\varphi_1(y_1,\ldots,y_d)}{\varphi_2(y_1,\ldots,y_d)}$$

and define the degree of $\varphi(y_1,\ldots,y_d)$, deg φ, to be max(deg φ_1,deg φ_2). To indicate partial derivatives of φ, we write $D_i\varphi$ for $\frac{\partial\varphi}{\partial y_i}$, $D_{i,j}\varphi$ for $\frac{\partial\varphi}{\partial y_i \partial y_j}$, etc., and let $D_i\varphi(\bar{y}_1,\ldots,\bar{y}_d)$ and $D_{i,j}\varphi(\bar{y}_1,\ldots,\bar{y}_d)$ denote the values of $D_i\varphi$ and $D_{i,j}\varphi$ at $(\bar{y}_1,\ldots,\bar{y}_d)$ respectively. The symbol x is also used as an indeterminant over I.

Let α be an algebraic number. α is called an <u>algebraic number of degree</u> r if

$$r = \min\{\deg s \mid s(x) \in I[x] \text{ and } s(\alpha) = 0\}.$$

We say α is a <u>rational number</u> if r=1 and α is a <u>quadratic irrational number</u> if r=2. $m(x) \in I[x]$ is called the <u>minimal polynomial</u> associated with α if $m(\alpha) = 0$, deg m = r and m(x) is monic.

Let $\{x_i\}$ be a sequence converging to α such that $e_i := |x_i-\alpha| \neq 0$ for all i. The sequence $\{x_i\}$ is of <u>order of convergence</u> p (or $\{x_i\}$ is a p^{th} order sequence) if

$$\lim_{i\to\infty} \frac{e_{i+1}}{e_i^{p-\epsilon}} = 0 \text{ and } \lim_{i\to\infty} \frac{e_{i+1}}{e_i^{p+\epsilon}} \neq 0$$

for any $\epsilon > 0$.

For each algebraic number α, define $G(\alpha)$ to be the class of all sequences $\{x_i\}$ with the following properties:

(i) $\lim_{i\to\infty} x_i = \alpha$ and $x_i \neq \alpha$ for all i,

(ii) $\{x_i\}$ has order $p > 1$,

(iii) <u>$\{x_i\}$ is generated by the iteration φ,</u> that is, for some $\varphi(y_1,\ldots,y_d) \in I(y_1,\ldots,y_d)$, $x_{i+1} = \varphi(x_i,\ldots,x_{i-d+1})$ for $i \geq d$, with $\alpha = \varphi(\alpha,\ldots,\alpha)$.

For any sequence $\{x_i\}$ in $G(\alpha)$ generated by the iteration φ, the <u>multiplication efficiency</u> of $\{x_i\}$ is defined as

$$E(\{x_i\}) = \frac{\log_2 p}{M}$$

by Kung [1], or as

$$\bar{E}(\{x_i\}) = \frac{\log_2 p}{\bar{M}}$$

by Paterson [3], where $M = M(\varphi)$, $\bar{M} = \bar{M}(\varphi)$ and p is the order of convergence of $\{x_i\}$. Obviously, we have $E(\{x_i\}) \le \bar{E}(\{x_i\})$. Define

$$\bar{E}(r) = \sup_{\alpha \in A(r)} \{ \sup_{\{x_i\} \in G(\alpha)} \bar{E}(\{x_i\}) \}$$

where $A(r)$ is the set of all algebraic numbers of degree r.

3. STATEMENT OF RESULTS

It follows from the results in Kung [1] that

$$(3.1) \quad \bar{E}(\{x_i\}) \le 1$$

(hence, $E(\{x_i\}) \le 1$) for any $\{x_i\} \in G(\alpha)$ and for any algebraic number α.

Theorem 1.

If α is an algebraic number of degree $r \ge 2$, then for any sequence $\{x_i\}$ in $G(\alpha)$ generated by the iteration φ,

$$(3.2) \quad \bar{M} \ge \log_2[r(\lceil p \rceil -1) + 1] - 1$$

or equivalently,

$$(3.3) \quad \bar{E}(\{x_i\}) \le (\log_2 p)/\{\log_2[r(\lceil p \rceil -1) + 1]-1\},$$

where $\bar{M} = \bar{M}(\varphi)$ and p is the order of convergence of $\{x_i\}$.

Since $(\log_2 p)/\{\log_2[r(\lceil p \rceil -1) + 1] - 1\} < 1$ whenever $r > 2$ and $p > 2$, (3.3) is a stronger result than (3.1). Moreover, (3.2) implies that if we fix p then $\bar{M} \ge \log_2 r + c$ for constant c. This means that to achieve the same order of convergence we have to use more multiplications or divisions, except by constants, in each iteration stage when the degree r of the algebraic number is higher.

Suppose that we only consider sequences $\{x_i\}$ of order of convergence $p \le U$ for some constant $U > 0$. (This is the case in practice.) Then (3.3) implies that

$$\bar{E}(r) = O[(\log r)^{-1}] \text{ as } r \to \infty.$$

However, Paterson [3] showed that

$$\bar{E}(r) \ge .82 r^{-\frac{1}{2}}$$

and conjectured that

$$\bar{E}(r) = O(r^{-\frac{1}{2}}) \text{ as } r \to \infty.$$

It is still an open problem to find how fast $\bar{E}(r)$ drops as $r \to \infty$.

Will $E(\{x_i\})$ or $\bar{E}(\{x_i\})$ achieve its upper bound of unity? Paterson [3] observed that for any quadratic irrational number α, there exists $\{x_i\} \in G(\alpha)$ such that $\bar{E}(\{x_i\}) = 1$. Kung [1] observed that for the rational number $-\frac{1}{2}$ there exists $\{x_i\} \in G(-\frac{1}{2})$ such that $E(\{x_i\}) = 1$.

Theorem 2.

Let α be an algebraic number of degree r and let $\{x_i\} \in G(\alpha)$. Then

$$(3.4) \quad r = 1 \text{ if } E(\{x_i\}) = 1;$$

$$(3.5) \quad r = 1 \text{ or } 2 \text{ if } \bar{E}(\{x_i\}) = 1.$$

Corollary 2.1.

(i) *α is a rational number if and only if there exists $\{x_i\} \in G(\alpha)$ with $E(\{x_i\}) = 1$.*

(ii) *α is a quadratic irrational number if and only if there exists $\{x_i\} \in G(\alpha)$ with $\bar{E}(\{x_i\}) = 1$ and there exists no $\{x_i\} \in G(\alpha)$ with $E(\{x_i\}) = 1$.*

Proof of Corollary 2.1.

(i) The sufficiency of the condition is already implied by Theorem 2. Let us therefore assume that α is a rational number. Define $\varphi(x) = (x-\alpha)^2 + \alpha$. Then clearly $\varphi(x) \in I(x)$,

$M(\varphi) = 1$ and the sequence $\{x_i\}$ generated by φ is of order of convergence $p=2$. Hence $E(\{x_i\}) = 1$.

(ii) The sufficiency of the condition is implied by (i) and Theorem 2. The necessity of the condition follows from (i) and Paterson's observation. QED

Corollary 2.1 answers completely the question of when $E(\{x_i\})$ or $\bar{E}(\{x_i\})$ achieves its optimal value of unity. In fact, Corollary 2.1 gives new characterization theorems for rational and quadratic irrational numbers.

4. PROOF OF THEOREM 1

Let us first establish three lemmas.

<u>Lemma 1.</u>

If $\Psi(x) \in I(x)$, $\Psi(x) \not\equiv 0$ and if $\Psi^{(i)}(\alpha) = 0$ for $i=0,\ldots,\ell-1$, for some algebraic number α of degree r, then

$$\Psi_1(x) = q(x) \cdot [m(x)]^{\ell}$$

for some $q(x) \in I[x]$, $q(x) \not\equiv 0$, where $m(x)$ is the minimal polynomial associated with α.

<u>Proof of Lemma 1.</u>

We prove the lemma by induction on ℓ. It is well known that any polynomial in $I[x]$ which has a zero at α is divisible by $m(x)$. Therefore, if $\ell=1$ then the statement of Lemma 1 is true. Assume that the statement is true for $\ell \le n$. Suppose that $\Psi^{(i)}(\alpha) = 0$ for $i=0,\ldots,n$. By the induction hypothesis $\Psi_1(x) = w(x) \cdot s(x)$ for some $w(x) \in I[x]$, $w(x) \not\equiv 0$, where $s(x) = [m(x)]^n$. Then $\Psi(x) = w(x) \cdot t(x)$ where $t(x) = \frac{s(x)}{\Psi_2(x)}$. Note that $\Psi^{(n)}(x) = \sum_{0\le i\le n} \binom{n}{i} w^{(n-i)}(x) \cdot t^{(i)}(x)$. But $\Psi^{(n)}(\alpha) = 0$ and $t^{(i)}(\alpha) = 0$ for $i=0,\ldots,n-1$. Thus, $w(\alpha)t^{(n)}(\alpha) = 0$. Using the fact that $m'(\alpha) \neq 0$ and $\Psi_2(\alpha) \neq 0$, one can easily verify that $t^{(n)}(\alpha) \neq 0$. Therefore $w(\alpha) = 0$. This implies that there exists $v(x) \in I[x]$ such that $w(x) = v(x) \cdot m(x)$. Thus, $\Psi_1(x)=v(x)\cdot[m(x)]^{n+1}$. Since $w(x) \not\equiv 0$, we have $v(x) \not\equiv 0$. The proof by induction is complete. QED

<u>Lemma 2.</u>

Let $\varphi(y_1,\ldots,y_d) \in I(y_1,\ldots,y_d)$. If φ generates a p^{th} order sequence in $G(\alpha)$ for some algebraic number α, then

$$(4.1) \quad \deg \varphi \ge \lceil p \rceil$$

and for any $k=1,\ldots,\lceil p\rceil-1$,

$$(4.2) \quad D_{i_1,\ldots,i_k}\varphi(\alpha,\ldots,\alpha) = 0$$

for all $1 \le i_1,\ldots,i_k \le d$.

<u>Proof of Lemma 2.</u>

Since (4.1) has been shown in Kung [1], we only prove (4.2). From Kung [1], we know that

$$(4.3) \quad \varphi_1(y_1,\ldots,y_d) - \alpha\varphi_2(y_1,\ldots,y_d) = \sum_{j_1+\cdots+j_d\ge\lceil p\rceil} c(j_1,\ldots,j_d)(y_1-\alpha)^{j_1}\cdots(y_d-\alpha)^{j_d}$$

where the constants $c(j_1,\ldots,j_d)$ are independent of $y_1,\ldots,y_d$. Since $D_{i_1,\ldots,i_k}\varphi = D_{i_1,\ldots,i_k}(\varphi-\alpha) = D_{i_1,\ldots,i_k}\left(\frac{\varphi_1-\alpha\varphi_2}{\varphi_2}\right)$, (4.2) follows from (4.3). QED

See Kung[1] for the proof of the following lemma.

<u>Lemma 3.</u>

If $\varphi(y_1,\ldots,y_d) \in I(y_1,\ldots,y_d)$, then

$$\bar{M}(\varphi) \ge \log_2(\deg \varphi).$$

Proof of Theorem 1.

Let $\{x_i\}$ be a p^{th} order sequence in $G(\alpha)$ generated by φ. Since $\varphi(\alpha,\ldots,\alpha) = \alpha$, there exists a neighborhood $N(\alpha,\ldots,\alpha)$ of $(\alpha,\ldots,\alpha)$ such that φ_2 does not vanish in $N(\alpha,\ldots,\alpha)$. Choose an open interval I_α containing α such that $I_\alpha \times \ldots \times I_\alpha \subseteq N(\alpha,\ldots,\alpha)$. Then we define a function $\Phi: I_\alpha \to R$ by $\Phi(x) = \varphi(x,\ldots,x)$. Φ is well-defined since $\varphi_2(x,\ldots,x) \neq 0$ for $x \in I_\alpha$. Clearly, $\Phi(x) \in I(x)$. Recall that $D_i\varphi$ denotes the partial derivative of φ with respect to y_i, and that $D_i\varphi(x,\ldots,x)$ denotes the value of $D_i\varphi$ evaluated at $(x,\ldots,x)$ for $x \in I_\alpha$. Suppose that $D_i\varphi(x,\ldots,x) \equiv 0$ for all $i=1,\ldots,d$. Then by the chain rule,

$$\frac{d}{dx}\Phi(x) \equiv \frac{d}{dx}\varphi(x,\ldots,x) \equiv \sum_{i\le i\le d} D_i\varphi(x,\ldots,x) \equiv 0$$

Hence Φ is a constant on I_α. Since $\Phi(\alpha) = \varphi(\alpha,\ldots,\alpha) = \alpha$,

$$\Phi(x) = \frac{\varphi_1(x,\ldots,x)}{\varphi_2(x,\ldots,x)} = \alpha$$

for all $x \in I_\alpha$. Choose a rational number $\bar{x}$ in I_α. Note that the polynomials $\varphi_i(x,\ldots,x)$, $i=1,2$, have integral coefficients. Hence $\frac{\varphi_1(\bar{x},\ldots,\bar{x})}{\varphi_2(\bar{x},\ldots,\bar{x})}$ is a rational number. This implies that α is a rational number. This is a contradiction. Therefore,

$$(4.4) \quad D_{i_1}\varphi(x,\ldots,x) \not\equiv 0$$

for some $1 \le i_1 \le d$. Now we define another function $\Psi: I_\alpha \to R$ by $\Psi(x) = D_{i_1}\varphi(x,\ldots,x)$. Clearly, $\Psi(x) \in I(x)$. By the chain rule, for $k=2,\ldots,\lceil p\rceil-1$,

$$\Psi^{(k-1)}(x) = \sum_{1\le i_2,\ldots,i_k\le d} D_{i_1,\ldots,i_k}\varphi(x,\ldots,x).$$

Then it follows from Lemma 2 that $\Psi^{(i)}(\alpha) = 0$ for $i=0,\ldots,\lceil p\rceil-2$. By (4.4) $\Psi(x) \not\equiv 0$. Hence it follows from Lemma 1 that $\deg \Psi_1 \ge (\lceil p\rceil-1)\cdot\deg m = r(\lceil p\rceil-1)$. But one can easily see that $\deg(D_{i_1}\varphi)_1 \ge \deg \Psi_1$ and $2\deg \varphi \ge \deg(D_{i_1}\varphi)_1 + 1$. Hence $\deg \varphi \ge [r(\lceil p\rceil-1) + 1]/2$. By Lemma 3, we have $\bar{M} \ge \log_2[r(\lceil p\rceil-1) + 1] - 1$. QED

5. PROOF OF THEOREM 2

We first establish two auxiliary theorems.

Theorem 3.

Let $\Phi(x) \in I(x)$, and let α be an algebraic number. If $\Phi(\alpha) = \alpha$ and $\Phi^{(i)}(\alpha) = 0$, $i=1,\ldots,p-1$, for $p \ge 2$, then

$$\Phi_1^{(i)}(\alpha) - \alpha\Phi_2^{(i)}(\alpha) = 0, \; i=0,\ldots,p-1.$$

Proof of Theorem 3.

We use induction on p. If $\Phi(\alpha) = \alpha$ and $\Phi'(\alpha) = 0$, then $\Phi_1(\alpha) - \alpha\Phi_2(\alpha) = 0$ and $\Phi_2(\alpha)\Phi_1'(\alpha) - \Phi_1(\alpha)\Phi_2'(\alpha) = 0$; hence $\Phi_1'(\alpha) - \alpha\Phi_2'(\alpha) = 0$. Therefore, the statement of Theorem 3 is true if p=2. Assume that the statement is true for $p \le n$. Suppose that $\Phi(\alpha) = \alpha$ and $\Phi^{(i)}(\alpha) = 0$ for $i=1,\ldots,n$. By Lemma 1

$$(5.1) \quad \Phi_2(x)\Phi_1'(x) - \Phi_1(x)\Phi_2'(x) = q(x)\cdot[m(x)]^n$$

for some $q(x) \in I[x]$, where $m(x)$ is the minimal polynomial associated with α. Note that

$$(5.2) \quad \frac{d^{n-1}}{dx^{n-1}}[\Phi_2(x)\Phi_1'(x)-\Phi_1(x)\Phi_2'(x)]$$
$$= \Phi_2(x)\Phi_1^{(n)}(x)-\Phi_1(x)\Phi_2^{(n)}(x)$$
$$+ \sum_{0\le i\le n-2}\binom{n-1}{i}[\Phi_2^{(n-1-i)}(x)\Phi_1^{(i+1)}(x)$$
$$- \Phi_1^{(n-1-i)}(x)\Phi_2^{(i+1)}(x)].$$

Using the fact that $m(\alpha) = 0$, from (5.1) and (5.2) we get that

$$(5.3) \quad \Phi_2(\alpha)\Phi_1^{(n)}(\alpha)-\Phi_1(\alpha)\Phi_2^{(n)}(\alpha)$$

$$+ \sum_{0\le i\le n-2} \binom{n-1}{i} [\Phi_2^{(n-1-i)}(\alpha)\Phi_1^{(i+1)}(\alpha) - \Phi_1^{(n-1-i)}(\alpha)\Phi_2^{(i+1)}(\alpha)] = 0.$$

But by the induction hypothesis,

$$\Phi_1^{(i)}(\alpha) - \alpha\Phi_2^{(i)}(\alpha) = 0, \quad i=0,\dots,n-1.$$

Hence, for $i=0,\dots,n-2$,

$$\Phi_2^{(n-1-i)}(\alpha)\Phi_1^{(i+1)}(\alpha)-\Phi_1^{(n-1-i)}(\alpha)\Phi_2^{(i+1)}(\alpha)$$
$$= \Phi_2^{(n-1-i)}(\alpha)[\Phi_1^{(i+1)}(\alpha)-\alpha\Phi_2^{(i+1)}(\alpha)]$$
$$= 0.$$

Therefore (5.3) implies that

$$\Phi_2(\alpha)\Phi_1^{(n)}(\alpha)-\Phi_1(\alpha)\Phi_2^{(n)}(\alpha) = 0,$$

and hence

$$\Phi_1^{(n)}(\alpha)-\alpha\Phi_2^{(n)}(\alpha) = 0.$$

The proof by induction is complete. QED

Theorem 4.

Let $\Phi(x) \in I(x)$. If $M(\Phi) = \log_2(\deg \Phi)$, then $\deg \Phi_2 < \deg \Phi_1 = 2^{M(\Phi)}$ and the leading coefficient of $\Phi_1(x)$ is divisible by that of $\Phi_2(x)$.

Proof of Theorem 4.

Consider the algorithm which computes $\Phi(x)$ in $M(\Phi) = \log_2(\deg \Phi)$ multiplications or divisions. Since by Lemma 3,

$$M(\Phi) \ge \bar{M}(\Phi) \ge \log_2(\deg \Phi),$$

we have $M(\Phi) = \bar{M}(\Phi)$. That is, there are no multiplications or divisions by constants in the algorithm. Note that $\deg \Phi = 2^{M(\Phi)}$. We prove the theorem by induction on $M = M(\Phi)$. It is easy to check that the statement of Theorem 4 is true if $M=1$. Assume that the statement is true for $M \le L$, and let us prove it for $M=L+1$. Suppose that $\deg \Phi = 2^{L+1}$ and $M(\Phi) = \log_2(\deg \Phi)$. Then $\Phi(x)$ can be computed in $(L+1)$ multiplications or divisions by some algorithm. With respect to this algorithm let $R_n(x)$ denote the result immediately following the n^{th} multiplication or division for $n=1,\dots,L+1$. Let $R_0(x) = x$. Then for $n=0,\dots,L$ either

$$(5.4) \quad R_{n+1}(x) = (\sum_{0\le i\le n} M_{n,i}R_i(x) + A_n) \cdot (\sum_{0\le i\le n} N_{n,i}R_i(x) + B_n)$$

or

$$(5.5) \quad R_{n+1}(x) = (\sum_{0\le i\le n} M_{n,i}R_i(x) + A_n) / (\sum_{0\le i\le n} N_{n,i}R_i(x) + B_n),$$

for some integers $M_{n,i}$, $N_{n,i}$ and some numbers A_n, B_n, for $i=0,\dots,n$; and

$$\Phi(x) = \sum_{0\le i\le L+1} M_{L+1,i}R_i(x) + A_{L+1}$$

for some integers $M_{L+1,i}$, $i=0,\dots,L+1$, and some number A_{L+1}. One can show that, for $n=1,\dots,L+1$, the following is true (see Kung [1]). For any integers $K_0,\dots,K_n$, and any number C,

$$\sum_{0\le i\le n} K_iR_i(x) + C = \frac{P_n(x;K,C)}{Q_n(x)},$$

where $P_n(x;K,C)$ is a polynomial in $I[x]$ depending on $K = (K_0,\dots,K_n)$ and on C; where $Q_n(x)$ is a polynomial in $I[x]$ independent of K and of C; moreover, both polynomials have degree $\le 2^n$. Now suppose that for $n=L$ (5.4) holds; that is,

$$(5.6) \quad R_{L+1}(x) = (\sum_{0\le i\le L} M_{L,i}R_i(x) + A_L) \cdot (\sum_{0\le i\le L} N_{L,i}R_i(x) + B_L).$$

Then

$$(5.7) \quad \Phi(x) = \sum_{0\le i\le L+1} M_{L+1,i}R_i(x) + A_{L+1}$$
$$= M_{L+1,L+1}R_{L+1}(x)+ \sum_{0\le i\le L} M_{L+1,i}R_i(x)+A_{L+1}$$
$$= \frac{P_{L+1}(x;M_{L+1},A_{L+1})}{Q_{L+1}(x)}$$

where

(5.8) $P_{L+1}(x;M_{L+1},A_{L+1})$
$= M_{L+1,L+1}\cdot P_L(x;M_L,A_L)\cdot P_L(x;N_L,B_L)$
$+ P_L(x;M_{L+1},A_{L+1})\cdot Q_L(x)$

and

(5.9) $Q_{L+1}(x) = [Q_L(x)]^2$.

Let $r(x)$ be the greatest common divisor of $P_L(x;M_L,A_L)$ and $Q_L(x)$. (Let $r(x) \equiv 1$ if $P_L(x;M_L,A_L)$ and $Q_L(x)$ are relatively prime.) Write $P_L(x;M_L,A_L) = r(x)\cdot p(x)$ and $Q_L(x) = r(x)\cdot q(x)$. Then from (5.7), (5.8), (5.9),

(5.10) $\Phi(x)$

$$= \frac{M_{L+1,L+1}\cdot p(x)\cdot P_L(x;N_L,B_L)+P_L(x;M_{L+1},A_{L+1})\cdot q(x)}{r(x)\cdot [q(x)]^2}$$

Suppose that $\deg(\sum_{0\le i\le L} M_{L,i}R_i + A_L) < 2^L$. Then $\deg p < 2^L$ and $\deg q < 2^L$. Note that if $r(x) \equiv 1$ then $\deg r\cdot q^2 < 2^{L+1}$ and on the other hand, if $\deg r > 1$ then $\deg r\cdot q^2 < \deg r^2\cdot q^2 = \deg Q_L^2 \le 2^{L+1}$. Therefore, $\deg r\cdot q^2 < 2^{L+1}$. Also note that since both $P_L(x;N_L,B_L)$ and $P_L(x;M_{L+1},A_{L+1})$ have degree $\le 2^L$, $M_{L+1,L+1}\cdot p(x)\cdot P_L(x;N_L,B_L) + P_L(x;M_{L+1},A_{L+1})\cdot q(x)$ has degree $< 2^{L+1}$. Hence (5.10) implies that $\deg \Phi < 2^{L+1}$. This is a contradiction. Therefore, $\deg(\sum_{0\le i\le L} M_{L,i}R_i + A_L) = 2^L$. Obviously, $\sum_{0\le i\le L} M_{L,i}R_i(x) + A_L$ can be computed in L multiplications or divisions. Hence by the induction hypothesis, $\deg Q_L < 2^L$, and $P_L(x;M_L,A_L)$ has degree 2^L and the leading coefficient of $P_L(x;M_L,A_L)$ is divisible by that of $Q_L(x)$. Similarly, we can prove that $P_L(x;N_L,B_L)$ has the same property. Therefore, from (5.7), (5.8), (5.9), we conclude that $\deg \Phi_2 < \deg \Phi_1 = 2^{L+1}$ and the leading coefficient of $\Phi_1(x)$ is divisible by that of $\Phi_2(x)$. Similarly, we can obtain the same conclusion if for n=L (5.5) holds; that is,

$$R_{L+1} = (\sum_{0\le i\le L} M_{L,i}R_i(x) + A_L)/(\sum_{0\le i\le L} N_{L,i}R_i(x) + B_L).$$

The proof by induction is complete. QED

Proof of Theorem 2.

Assume that $\{x_i\}$ be a p^{th} order sequence generated by φ, for some $\varphi(y_1,\ldots,y_d) \in I(y_1,\ldots,y_d)$. Define $\Phi: I_\alpha \to R$ by $\Phi(x) = \varphi(x,\ldots,x)$ for some open interval I_α containing α, as in the previous section. Then by the chain rule,

$$\Phi^{(k)}(x) = \sum_{1\le i_1,\ldots,i_k\le d} D_{i_1,\ldots,i_k}\varphi(x,\ldots,x)$$

for any positive integer k, Hence by Lemma 2 we have

(5.11) $\Phi^{(k)}(\alpha) = 0,\ k=1,\ldots,\lceil p\rceil-1$.

We first prove (3.5). Assume that $\bar{E}(\{x_i\}) = 1$. Suppose that $r > 2$. Since by (3.3) $\bar{E}(\{x_i\}) < 1$ whenever $r > 2$ and $p > 2$, we have $p \le 2$. Hence $1 \le \bar{M}(\varphi) = \log_2 p \le 1$. This implies that $\bar{M}(\varphi) = 1$ and p=2. Since $\bar{M}(\varphi) = 1$, one can easily see that $\deg \varphi_1 = 2$ and $\deg \varphi_2 \le 1$. Hence $\varphi_1(x,\ldots,x) - x\varphi_2(x,\ldots,x)$ has degree at most 2. Suppose that $\varphi_1(x,\ldots,x) - x\varphi_2(x,\ldots,x) \equiv 0$. Then $\Phi(x) \equiv x$ and $\Phi'(x) \equiv 1$. But by (5.11) $\Phi'(\alpha) = 0$, since p=2. This contradiction shows that $\varphi_1(x,\ldots,x) -x\varphi_2(x,\ldots,x) \not\equiv 0$. Note that $\varphi(\alpha,\ldots,\alpha) = \alpha$, that is, $\varphi_1(\alpha,\ldots,\alpha) - \alpha\varphi_2(\alpha,\ldots,\alpha) = 0$. Therefore, α is a zero of the polynomial $\varphi_1(x,\ldots,x)-x\varphi_2(x,\ldots,x)$ which has degree one or degree two. This implies that $r \le 2$. Hence we get a contradiction by assuming that $r > 2$. Therefore $r \le 2$. We have shown (3.5).

Now suppose that $E(\{x_i\}) = 1$. Then $\bar{E}(\{x_i\}) =1$, and r=1 or 2 by (3.5). Suppose that r=2. From Lemma 2 and Lemma 3,

$$M(\varphi) \geq \bar{M}(\varphi) \geq \log_2(\deg \varphi) \geq \log_2\lceil p \rceil \geq \log_2 p.$$

But $E(\{x_i\}) = 1$, that is, $M(\varphi) = \log_2 p$. We have

$$(5.12)\quad M(\varphi) = \bar{M}(\varphi) = \log_2(\deg \varphi) = \log_2\lceil p \rceil = \log_2 p.$$

Hence p is a integer. Now consider Φ. Clearly $\Phi(\alpha) = \alpha$. By Theorem 3, (5.11) implies that

$$(5.13)\quad \Phi_1^{(p-1)}(\alpha) - \alpha\Phi_2^{(p-1)}(\alpha) = 0.$$

Using the proof of Theorem 2, one can show that $\deg \Phi \geq \frac{2(p-1)+1}{2} = p-\frac{1}{2}$. But by (5.12) $p = \deg \varphi$. Hence $p = \deg \varphi \geq \deg \Phi \geq p-\frac{1}{2}$. This implies that $\deg \Phi = p$.

Note that the algorithm which computes $\varphi(y_1,\ldots,y_d)$ in $M(\varphi)$ multiplications or divisions reduces to an algorithm which computes $\Phi(x)$ in at most $M(\varphi)$ multiplications or divisions. Hence

$$M(\Phi) \leq M(\varphi) = \log_2 p = \log_2(\deg \Phi).$$

By Lemma 2, $M(\Phi) \geq \log_2(\deg \Phi)$. Thus $M(\Phi) = \log_2(\deg \Phi)$. Hence by Theorem 4, $\deg \Phi_2 \leq p-1$ and $\deg \Phi_1 = p$. Now suppose that

$$(5.14)\quad \Phi_1^{(p-1)}(x) - x\Phi_2^{(p-1)}(x) \equiv 0$$

Then $\deg \Phi_2 = p-1$. Let us assume that $\Phi_1(x) = \sum_{0\leq i\leq p} a_i x^i$ and $\Phi_2(x) = \sum_{0\leq i\leq p-1} b_i x^i$. Then by (5.14) we have $pa_p = b_{p-1}$. Note that $p = 2^{M(\varphi)} \geq 2$. This is a contradiction, since by Theorem 4 a_p is divisible by b_{p-1}. Hence,

$$\Phi_1^{(p-1)}(x) - x\Phi_2^{(p-1)}(x) \not\equiv 0.$$

Clearly, $\Phi_1^{(p-1)}(x) - x\Phi_2^{(p-1)}(x)$ is a polynomial of degree one. Hence (5.13) implies that α is a root of the linear equation $\Phi_1^{(p-1)}(x) - x\Phi_2^{(p-1)}(x) = 0$. Therefore, by assuming r=2 we have obtained r=1. This is a contradiction. Nevertheless, since r is either 1 or 2, we have thereby shown that r=1. QED

REFERENCES

[1] Kung, H. T., "A Bound on the Multiplication Efficiency of Iteration," Proceedings of the Fourth Annual ACM Symposium on Theory of Computing. To appear in Journal of Computer and System Sciences, 1973.

[2] Kung, H. T. and Traub, J. F., Computational Complexity of One-Point and Multipoint Iteration, report, Department of Computer Science, Carnegie-Mellon University, 1973.

[3] Paterson, M. S., "Efficient Iterations for Algebraic Numbers," in Complexity of Computer Computations, R. Miller and J. W. Thatcher (eds.), Plenum Press, New York, 1972, 44-52.

ACKNOWLEDGMENT

The author thanks R. I. Pelletier for reading over a draft of this paper.