MATHEMATICS OF COMPUTATION, VOLUME 26, NUMBER 119, JULY, 1972

A Continued Fraction Algorithm for Real Algebraic Numbers*

By David G. Cantor, Paul H. Galyean and Horst G. Zimmer

Abstract. Let α denote a real algebraic number that is a root of a polynomial $f(x) \in \mathbf{Z}[x]$. The purpose of this paper is to state an algorithm for finding the simple continued fraction expansion of α. Furthermore, an application of the algorithm to sign determination in real algebraic number fields is given.

1. Introduction. The task of constructively computing the simple continued fraction expansion (see [2]) for a real root α of a polynomial

$$f(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m \qquad (b_0 \neq 0)$$

over the rational integers $\mathbf{Z}$ raises no essential difficulties provided that α is the sole real root of $f(x)$. However, if $f(x)$ happens to have more than one real root, the problem arises of discriminating between the continued fraction expansion of α and of the other real roots of $f(x)$.

An attempt to solve this problem was made by Zassenhaus [5], who showed that, after a finite number of steps, the so-called "reduced state" of the continued fraction expansion of α (see below) is reached. (See also [2].) From there on, the discrimination of the real roots is automatically guaranteed. Unfortunately, no indication is given in Zassenhaus' method as to when the reduced state will be attained for a given α, nor does there seem to exist a simple device for achieving that state (cf. [6]). Nonetheless, a computer program was written by Smith [3] in which the method is applied to some special cases.

2. The Continued Fraction Algorithm. In this paper, we describe a different continued fraction algorithm that furnishes a solution to the discrimination problem mentioned above and that, moreover, appears to be much simpler than the routine designed by Zassenhaus [5].

Let us first remark that, as Zassenhaus [5] observed, it is expedient to reduce $f(x)$ to a polynomial having no multiple factors. We can eliminate them by replacing $f(x)$ by the polynomial $f(x)/(f(x), f'(x))$. In the trivial case in which α is a *rational* root of $f(x)$, the algorithm will simply terminate after a finite number of steps.

We confine ourselves therefore to giving a description of the algorithm as applied to an *irrational* real root α of the (not necessarily irreducible) polynomial $f(x)$ in $\mathbf{Z}[x]$.

Received January 18, 1971, revised December 6, 1971.

AMS 1970 *subject classifications.* Primary 10A30, 10F20; Secondary 12D10.

Key words and phrases. Continued fraction expansion, algorithm, discrimination of roots, irrational real algebraic numbers, *PV* numbers, binary search procedure, sign determination, mean value theorem.

* This research was supported in part by the Sloan Foundation and NSF Grants GP-23113 and GP-29074.

The polynomial $f(x)$ may, moreover, be supposed to have no rational roots at all. The continued fraction expansion of α is then calculated assuming that α is isolated by rational numbers (or infinity) r and s; i.e., α is the unique root of $f(x)$ in the closed interval $[r, s]$. Put $r_0 = r$, $s_0 = s$, and define the *0th successor* α_0 of α by

$$\alpha_0 = \alpha,$$

the *0th partial denominator* a_0 of α by

$$a_0 = [\alpha_0],$$

where [ ] designates the greatest integer function, and the *0th successor polynomial* $f_0(x)$ of $f(x)$ by

$$f_0(x) = f(x).$$

We have $f_0(\alpha_0) = 0$.

Let us assume by induction that, for an integer $n \geqq 1$, α_{n-1} is an irrational real root of a polynomial

$$f_{n-1}(x) = b_{0,n-1}x^m + b_{1,n-1}x^{m-1} + \cdots + b_{m,n-1}$$
$$(b_{0,n-1} \neq 0),\ (b_{i,0} = b_i \text{ for } 0 \leqq i \leqq m),$$

over $\mathbf{Z}$ having neither multiple factors nor rational roots, and that α_{n-1} is the unique root of $f_{n-1}(x)$ in the closed interval $[r_{n-1}, s_{n-1}]$.

Next, put $a_{n-1} = [\alpha_{n-1}]$, and let

$$\begin{aligned} r_n &= (s_{n-1} - a_{n-1})^{-1} && \text{if } s_{n-1} < a_{n-1} + 1, \\ &= 1 && \text{otherwise}, \\ s_n &= (r_{n-1} - a_{n-1})^{-1} && \text{if } r_{n-1} > a_{n-1}, \\ &= \infty && \text{otherwise}. \end{aligned}$$

Define the *nth successor* α_n of α by

$$\alpha_n = (\alpha_{n-1} - a_{n-1})^{-1},$$

the *nth partial denominator* a_n of α by

$$a_n = [\alpha_n],$$

and the *nth successor polynomial* $f_n(x)$ of $f(x)$ by

$$f_n(x) = x^m f_{n-1}(x^{-1} + a_{n-1}).$$

Clearly, $f_n(x)$ is a polynomial over $\mathbf{Z}$ having neither multiple factors nor rational roots, and α_n is one of the irrational real roots of $f_n(x)$. Moreover, α_n is the unique root of $f_n(x)$ in the closed interval $[r_n, s_n]$. Note that for $n \geqq 1$, we have $\alpha_n > 1$ and $1 \leqq r_n < s_n \leqq \infty$.

The definition of r_n, s_n and α_n leads us to the following observation which is of significance for the discrimination problem mentioned at the beginning (cf. [2] and the Theorem of Vincent [4]).

THEOREM. *Under the above hypothesis on α, r, and s, there exists n_1 such that, for all $n \geqq n_1$, we have*

$$r_n = 1 \quad \textit{and} \quad s_n = \infty .$$

Proof. The assertion results from two facts that are immediate consequences of the definition of r_n, s_n and α_n.

(1) If $r_n = 1$ *or* $s_n = \infty$ for some integer $n \geqq 1$, then it follows that

$r_{n+i} = 1$ for all even *or* all odd natural numbers i,
respectively,

and that

$s_{n+j} = \infty$ for all odd *or* all even natural numbers j,
respectively.

(2) For all integers $n \geqq 1$, the following hold:

$$\textit{either } r_n = 1 \textit{ or } a_{n-1} = [s_{n-1}]$$

and

$$\textit{either } s_n = \infty \textit{ or } a_{n-1} = [r_{n-1}].$$

Once we have arrived at an index $n_1 \geqq 1$ such that $r_{n_1} = 1$ and $s_{n_1} = \infty$, statement (1) implies that $r_n = 1$ and $s_n = \infty$ for all $n \geqq n_1$. To see that n_1 exists, consider the sequences $S = \{[r_0], [s_1], [r_2], \cdots\}$ and $T = \{[s_0], [r_1], [s_2], \cdots\}$, which are initially the continued fraction expansions of r and s, respectively. By (2), S and T must each eventually differ from the continued fraction expansion $\{a_0, a_1, a_2, \cdots\}$ of α since $r \neq \alpha$ and $s \neq \alpha$. S and T each then become $\{\cdots, 1, \infty, 1, \infty, \cdots\}$.

The actual determination of the partial denominators a_n of α can now be carried through in the following manner (see also [5]).

First, we find improved bounds for the irrational real root α_n of $f_n(x)$ where $n \geqq 0$. To this end, we have to introduce the set

$$\alpha_n = \alpha_n^{(1)}, \alpha_n^{(2)}, \cdots, \alpha_n^{(m)}$$

of the complex roots of $f_n(x)$. We recall that these roots can be defined inductively by setting $\alpha_0^{(i)} = \alpha^{(i)}$ and, for $n \geqq 1$,

$$\alpha_n^{(i)} = (\alpha_{n-1}^{(i)} - a_{n-1})^{-1} \qquad (i = 1, 2, \cdots, m).$$

Also, we use the *nth convergent* of the continued fraction expansion of α, that is, the fraction (see [2])

$$[a_0, a_1, \cdots, a_n] = p_n/q_n \qquad (p_n, q_n \in \mathbf{Z}).$$

As usual, define $p_{-1} = 1$ and $q_{-1} = 0$.

The integers p_{n-1}, p_{n-2} and q_{n-1}, q_{n-2} ($n \geqq 1$) appear in the formula connecting $\alpha^{(i)}$ with $\alpha_n^{(i)}$, namely,

$$\alpha^{(i)} = (p_{n-1}\alpha_n^{(i)} + p_{n-2})/(q_{n-1}\alpha_n^{(i)} + q_{n-2}) \qquad (i = 1, 2, \cdots, m)$$

or, conversely,

$$\alpha_n^{(i)} = -(q_{n-2}\alpha^{(i)} - p_{n-2})/(q_{n-1}\alpha^{(i)} - p_{n-1}).$$

We write the latter relation for $n \geqq 2$ in the form

$$\alpha_n^{(i)} = -\frac{\alpha^{(i)} - p_{n-2}/q_{n-2}}{\alpha^{(i)} - p_{n-1}/q_{n-1}} \cdot \frac{q_{n-2}}{q_{n-1}} \qquad (i = 1, 2, \cdots, m).$$

Noting that $p_{n-2}/q_{n-2} \to \alpha$ and $p_{n-1}/q_{n-1} \to \alpha$, as $n \to \infty$, and that $\alpha \neq \alpha^{(i)}$ for all i in the interval $1 < i \leqq m$, we conclude that, for $i \neq 1$ and for all large n, the $|\alpha_n^{(i)}|$ are asymptotic to q_{n-2}/q_{n-1}. On the other hand, it follows from the second of the two relations

$$\begin{aligned} p_{n-1} &= p_{n-2}a_{n-1} + p_{n-3} \\ q_{n-1} &= q_{n-2}a_{n-1} + q_{n-3} \end{aligned} \qquad (n \geqq 2),$$

or, respectively, from the definition of q_{-1} and q_0 that

$$q_{n-2}/q_{n-1} \leqq a_{n-1}^{-1} \qquad (n \geqq 2)$$

with strict inequality for $n \geqq 3$. For all large n, the conjugates $\alpha_n^{(i)}$ of $\alpha_n = \alpha_n^{(1)}$ satisfy

$$|\alpha_n^{(i)}| < a_{n-1}^{-1} \qquad (1 < i \leqq m).$$

It is clear from the above relations that there exists n_2 such that, for all $n \geqq n_2$, the following two conditions are fulfilled:

$$\begin{aligned} &\alpha_n > 1, \\ &0 < -\operatorname{Re}(\alpha_n^{(i)}) \leqq |\alpha_n^{(i)}| < 1 \qquad (1 < i \leqq m), \end{aligned}$$

where "Re" denotes the real part of a complex number. This is what Zassenhaus [5] calls the *reduced state* of the continued fraction expansion of α. Thus, for all large n, α_n is a *PV* number.

As soon as the reduced state is reached, we know, because of the relation

$$\sum_{i=1}^{m} \alpha_n^{(i)} = -b_{1,n}/b_{0,n}$$

on the roots $\alpha_n^{(i)}$ of $f_n(x)$, that $\alpha_n = \alpha_n^{(1)}$ lies in the interval

$$-b_{1,n}/b_{0,n} < \alpha_n < (m - 1) - b_{1,n}/b_{0,n}.$$

The upper bound for α_n can be further improved. Specifically, from the relations derived above, we infer that α_n is asymptotic to $(m - 1)q_{n-2}/q_{n-1} - b_{1,n}/b_{0,n}$ and moreover, that there exists n_3 such that, for all $n \geqq n_3$, we have

$$\alpha_n < (m - 1)/a_{n-1} - b_{1,n}/b_{0,n}.$$

Now, if $n \geqq 1$ and $a_0, a_1, \cdots, a_{n-1}$ are already computed, we calculate a_n via a modified binary search process in the interval $u_n \leqq a_n \leqq v_n$ which is roughly defined as follows. Put

$$n_4 = \max\{n_1, n_2, n_3\},$$

where n, are the preceding index bounds. Then, we put for $n < n_4$,

$$\begin{aligned} u_n &= [r_n] \quad \text{if } n \text{ is even}, \\ &= [s_n], \quad \text{if } n \text{ is odd}, \end{aligned}$$

$$\begin{aligned} v_n &= \min\{[s_n], [t_n]\}, \quad \text{if } n \text{ is even,} \\ &= \min\{[r_n], [t_n]\}, \quad \text{if } n \text{ is odd,} \end{aligned}$$

where

$$t_n = 1 + \max_{1 \leqq i \leqq m}\{|b_{i,n}|/|b_{0,n}|\},$$

and, for $n \geqq n_4$,

$$\begin{aligned} u_n &= \max\{1, [-b_{1,n}/b_{0,n}]\}, \\ v_n &= [(m - 1)/a_{n-1} - b_{1,n}/b_{0,n}]. \end{aligned}$$

Note that, for $n \geqq 1$, u_n and v_n are positive integers.

The nth partial denominator a_n of α is then determined as the unique natural number λ_n in the interval $u_n \leqq \lambda_n \leqq v_n$ for which

$$\operatorname{sgn} f_n(\lambda_n) \neq \operatorname{sgn} f_n(\lambda_n + 1).$$

Before describing the binary search process for a_n, we note that, if $n \geqq n_4$, it is expedient to precede the binary search with the sign test for

$$\lambda_n = [(m - 1)q_{n-2}/q_{n-1} - b_{1,n}/b_{0,n}],$$

because the number in square brackets is, as we have seen, a good approximation to α_n. This, of course, requires computation of the q_n. If $\operatorname{sgn} f_n(\lambda_n) \neq \operatorname{sgn} f_n(\lambda_n + 1)$ for this λ_n, then $a_n = \lambda_n$. Otherwise, we start the binary search as follows. We put $\lambda_n = v_n$ and check whether $\operatorname{sgn} f_n(\lambda_n) \neq \operatorname{sgn} f_n(\lambda_n + 1)$. If so, then $a_n = v_n$. If not, we know that $u_n \leqq a_n \leqq v_n - 1$. Unless $u_n = v_n - 1$, in which case $a_n = u_n$, we put

$$w_n = [\tfrac{1}{2}(u_n + v_n)]$$

and compare the signs of $f_n(w_n)$ and $f_n(v_n)$, say. If they differ, we replace u_n by w_n; otherwise, we leave u_n unchanged and substitute w_n for v_n. The search process is then repeated (if need be) with respect to the new interval, until $u_n = v_n - 1$.

This algorithm has been implemented as a computer program which we shall use to build the example of Section 4.

3. An Application of the Algorithm to Sign Determination. In this section, we shall outline a method for performing sign determination in a real algebraic number field

$$K = \mathbf{Q}(\alpha)$$

over the field of rational numbers $\mathbf{Q}$, where α is an irrational real root of a (not necessarily irreducible) polynomial $f(x)$ in $\mathbf{Z}[x]$ of degree $m > 1$ as before. This method seems to be somewhat simpler than the one proposed by Kempfert [1] and Zassenhaus [6]; however, their method applies to any ordered field.

Every element $\beta \in K$ can be represented in the form $\beta = g(\alpha)$ with a polynomial $g(x)$ in $\mathbf{Q}[x]$ of degree $<m$.

First of all, we may assume that $g(\alpha) \neq 0$, since if $g(\alpha)$ were 0, then $(f(x), g(x)) \neq 1$.

To determine the sign of $g(\alpha)$, we employ the continued fraction algorithm of Section 2 in order to approximate α by its convergents p_n/q_n. The theory of continued fractions yields, for the approximation of α by p_n/q_n, the estimate (see [2])

$$|\alpha - p_n/q_n| < 1/q_n^2,$$

where $q_n \to \infty$, as $n \to \infty$.

We shall show that, for all large n, the sign of $g(\alpha)$ can be obtained from the relation

$$\operatorname{sgn} g(\alpha) = \operatorname{sgn} g(p_n/q_n).$$

To this end, we note that, by the mean value theorem (cf. [6]), the formula

$$g(\alpha) - g(p_n/q_n) = g'(\xi)(\alpha - p_n/q_n)$$

is valid, where $g'(x)$ denotes the derivative of $g(x)$ and ξ is a real number lying between α and p_n/q_n. Let M be a bound for $g'(x)$ for x, say between p_0/q_0 and p_1/q_1. We thus have

$$|g(\alpha) - g(p_n/q_n)| < M/q_n^2.$$

Then $g(p_n/q_n) \to g(\alpha)$. For large enough n, $|g(p_n/q_n)| \geqq M/q_n^2$ and then $\operatorname{sgn} g(p_n/q_n) = \operatorname{sgn} g(\alpha)$.

4. An Example for the Continued Fraction Algorithm. We compute here the continued fraction expansion for three roots of the polynomial

$$f(x) = x^7 - 7x + 3,$$

which has three irrational real roots and four complex roots.

In the table which follows, the first column contains n, the second, third, and fourth contain the a_n for the three real roots $\alpha^{(1)} \sim -1.444 \cdots$, $\alpha^{(2)} \sim 0.429 \cdots$, $\alpha^{(3)} \sim 1.233$.

n	$\alpha^{(1)}$	$\alpha^{(2)}$	$\alpha^{(3)}$
0	−2	0	1
1	1	2	3
2	1	3	2
3	3	53	2
4	1	5	4
5	86	1	15
6	63	2	4
7	1006	1	1
8	2	1	7
9	1	1	70
10	3	1	1
11	3	91	7
12	2	1	2
13	3	1	1
14	1	1	8
15	1	5	4

Department of Mathematics
University of California
Los Angeles, California 90024

Department of Mathematics
University of California
Los Angeles, California 90024

Universität Karlsruhe (TH)
Mathematisches Institut II
75 Karlsruhe 1
Germany

1. H. Kempfert, "On sign determinations in real algebraic number fields," *Numer. Math.*, v. 11, 1968, pp. 170–174. MR **37** #1355.

2. J. Lagrange, "Sur la résolution des équations numériques," *Oeuvres.* Vol. 2, pp. 560–578.

3. D. L. Smith, *The Calculation of Simple Continued Fraction Expansions of Real Algebraic Numbers*, Master Thesis, Ohio State University, Columbus, Ohio, 1969.

4. J. V. Uspensky, *Theory of Equations*, McGraw-Hill, New York-Toronto-London, 1948.

5. H. Zassenhaus, *On the Continued Fraction Development of Real Irrational Algebraic Numbers*, Ohio State University, Columbus, Ohio, 1968. (Unpublished.)

6. H. Zassenhaus, "A real root calculus," *Computational Problems in Abstract Algebra*, edited by J. Leech, Pergamon, Oxford, 1970.