AN ALGORITHM FOR HALTER-KOCH UNITS

Leon Bernstein

Dedicated to James M. Vaughn, Jr.

INTRODUCTION

In a most remarkable paper Halter-Koch [6] gives the following abstract of his results (translated from German): "By means of the Modified Jacobi-Perron Algorithm, Bernstein, Hasse and Stender have constructed a system of independent units for some (infinite) classes of totally real algebraic number fields; they have shown that in certain cases (for infinitely many algebraic fields of degree $n = 3, 4, 6$) this system represents a basis of fundamental units or how such a basis can be obtained from the system. In the present paper I shall disclose maximal independent systems of units for a much wider class of algebraic number fields. Whether these units can again be obtained from an algorithm, and in which cases they turn out to be fundamental, is subject to further investigations." (The remarks in parentheses were added by the author.)

In this paper the author will solve the first of the two challenging problems posed by Halter-Koch: he will construct an algorithm by means of which he will obtain all the units found by Halter-Koch.

It must be emphatically mentioned that the Jacobi-Perron [7], [8] algorithm or its modification as used by the author [2] are especially significant when they become periodic. The author succeeded in disclosing a few classes of infinitely many algebraic number fields of any degree $n \geq 2$, a proper basis of which becomes periodic by the Jacobi-Perron algorithm or its generalization [1], [2]; on the basis of an important theorem by Hasse and the author [5], units from these algorithms which were in some cases a maximal independent system of units; Stender [9] has proved that for these fields of degree $n = 3, 4, 6$ this forms a system of fundamental units. The author will prove that the above theorem for units holds also for the new algorithm exposed in the next chapter.

1. THE ZERO ALGORITHM

Though this differs in its structure from the Jacobi-Perron Algorithm [7], [8] and the Modified Jacobi-Perron Algorithm, as introduced by the author [1], [2], it preserves the same basic properties which will therefore be enumerated, but not proved here. Their proof is exclusively based on induction.

Definition. Let $F(x)$ be an n-th degree polynomial in one variable x over the field A of algebraic numbers, *viz.*

Received November 18, 1977.

Michigan Math. J. 25 (1978).

(1.1) $$F(x) = x^n + K_1 x^{n-1} + \dots + K_{n-1}x - d;$$
$$n \geq 2;\ K_i, d \in A\ (i = 1, \dots, n-1);\ d \neq 0;\ \pi_{i=1}^{n-1} K_i \neq 0.$$

Let

(1.2) $$F(w) = 0.$$

Hence $w^{-1} = d^{-1}(w^{n-1} + K_1 w^{n-2} + \dots + K_{n-2}w + K_{n-1}))$. Let

(1.3) $$a^{(0)} = (a_1^{(0)}(w), a_2^{(0)}(w), \dots, a_{n-1}^{(0)}(w)) = (a_1^{(0)}, a_2^{(0)}, \dots, a_{n-1}^{(0)}),$$
where the $a_i^{(0)}(w)$ are polynomials in w over A, and
$$1 \leq \deg a_i^{(0)}(w) \leq n-1,\ (i = 1, \dots, n-1),$$

be a properly chosen $n-1$ dimensional vector. The sequence $\langle a^{(v)} \rangle_{v=0,1}$ is called *the zero algorithm of the vector* $a^{(0)}$, if

(1.4) $$a^{(v+1)} = (a_1^{(v)} - b_1^{(v)})^{-1}(a_2^{(v)} - b_2^{(v)}, \dots, a_{n-1}^{(v)} - b_{n-1}^{(v)}, 1);$$
$$\text{where } a_1^{(v)} \neq b_1^{(v)};\ b_i^{(v)} = a_i^{(v)}(0); \qquad i = 1, \dots, n-1;\ v = 0,1, \dots .$$

The vectors $b^{(v)} = (b_1^{(v)}, \dots, b_{n-1}^{(v)})$ are called the companion vectors of $a^{(v)}$. The zero algorithm (abbreviated ZA) is called *periodic* if there exist minimal rational integers $L \geq 0$, $m \geq 1$ such that $a^{(m+v)} = a^{(v)}$, $v = L, L+1, \dots$; it is called *purely* periodic if $L = 0$. The sequence $\langle a^{(v)} \rangle$, $v = 0,1, \dots, L-1$ is called the *primitive preperiod,* $\langle a^{(v)} \rangle$, $v = L, L+1, \dots, L+m-1$, the *primitive period.*

The basic properties of the ZA are derived from sequences of numbers $A_i^{(v)}$, $(i = 0,1, \dots, n-1;\ v = 0,1, \dots)$ obtained from recursion formulas, as follows

(1.5) $$A_i^{(j)} = \delta_i^{(j)}, \qquad i,j = 0,1, \dots, n-1, \text{ the Kronecker delta,}$$

(1.6) $$A_i^{(v+n)} = A_i^{(v)} + \sum_{j=0}^{n-1} b_j^{(v)} A_i^{(v+j)}, \qquad i = 0,1, \dots, n-1.$$

(1.7) $$\begin{vmatrix} A_0^{(v)} & A_1^{(v)} \dots & A_{n-1}^{(v)} \\ A_0^{(v+1)} & A_1^{(v+1)} \dots & A_{n-1}^{(v+1)} \\ & & \\ A_0^{(v+n-1)} & A_1^{(v+n-1)} \dots & A_{n-1}^{(v+n-1)} \end{vmatrix} = (-1)^{v(n-1)}, \qquad v = 0,1, \dots .$$

(1.8) $$a_i^{(0)} = \frac{A_i^{(v)} + \sum_{j=1}^{n-1} a_j^{(v)} A_i^{(v+j)}}{A_0^{(v)} + \sum_{j=1}^{n-1} a_j^{(v)} A_0^{(v+j)}}; \qquad v = 0,1, \dots ,$$

(1.9) $$\prod_{i=1}^{v} a_{n-1}^{(i)} = A_0^{(v)} = \sum_{j=1}^{n-1} a_j^{(v)} A_0^{(v+j)}; \qquad v = 1,2, \dots ,$$

$$(1.10)\qquad \begin{vmatrix} 1 & A_0^{(v+1)} \dots & A_0^{(v+n-1)} \\ a_1^{(0)} & A_1^{(v+1)} \dots & A_1^{(v+n-1)} \\ a_2^{(0)} & A_2^{(v+1)} \dots & A_2^{(v+n-1)} \\ \vdots & \vdots & \vdots \\ a_{n-1}^{(0)} & A_{n-1}^{(v+1)} \dots & A_{n-1}^{(v+n-1)} \end{vmatrix} = \frac{(-1)^{v(n-1)}}{A_0^{(v)} + \sum_{j=1}^{n-1} a_j^{(v)} A_0^{(v+j)}}; \qquad v = 0,1, \dots .$$

We shall now give an example of a periodic ZA which will prove to be decisive for the further solution of our problem. We prove

THEOREM 1. *Let*

$$(1.11)\qquad \begin{gathered} f(x) = x^n + dt_1 x^{n-1} + \dots + dt_{n-1}x - d; \qquad (n = 2,3, \dots) \\ d,t_i \in A(i = 1, \dots, n-1);\ d \neq 0;\ \prod_{i=1}^{n-1} t_i \neq 0. \\ f(w) = 0;\ w^{-1} = d^{-1}(w^{n-1} + dt_1 w^{n-2} + \dots + dt_{n-1}). \end{gathered}$$

Further, let

$$(1.12)\qquad a^{(0)} = (w + dt_1, w^2 + dt_1 w + dt_2, \dots, w^{n-1} + dt_1 w^{n-2} + \dots + dt_{n-1}).$$

Then the ZA *of* $a^{(0)}$ *is purely periodic. The length of the primitive period,* m, *is* n *for* $a \neq 1$, *and* 1 *for* $a = 1$.

Proof. The following relation is obvious

$$(1.13)\qquad \begin{gathered} a^{(0)} - dt_i = w^i + dt_1 w^{i-1} + \dots + dt_{i-1} w = wa_{i-1}^{(0)}; \\ i = 2, \dots, n-1;\ a_1^{(0)} - dt_1 = w. \end{gathered}$$

By definition of the ZA, we obtain from (1.12)

$$(1.14)\qquad b^{(0)} = (dt_1, dt_2, \dots, dt_{n-1}),$$

hence

$$(1.15)\qquad a^{(0)} - b^{(0)} = (w, wa_1^{(0)}, \dots, wa_{n-1}^{(0)}),$$

$$(1.16)\qquad a^{(1)} = (a_1^{(0)}, a_2^{(0)}, \dots, a_{n-2}^{(0)}, d^{-1}a_{n-1}^{(0)}),$$

$$(1.17)\qquad b^{(1)} = (dt_1, dt_2, \dots, dt_{n-2}, t_{n-1}).$$

Completely analogously we obtain

$$(1.18)\qquad a^{(2)} = (a_1^{(0)}, \dots, a_{n-3}^{(0)}, d^{-1}a_{n-2}^{(0)}, d^{-1}a_{n-1}^{(0)}),$$

(1.19) $$b^{(2)} = (dt_1, \ldots, dt_{n-3}, t_{n-2}, t_{n-1}),$$

and generally

(1.20) $$a^{(i)} = (a_1^{(0)}, \ldots, a_{n-i-1}^{(0)}, d^{-1}a_{n-i}^{(0)}, \ldots, d^{-1}a_{n-1}^{(0)}),$$
$$b^{(i)} = (dt_1, \ldots, dt_{n-i-1}, t_{n-i}, \ldots, t_{n-1}), \qquad i = 1, \ldots, n-2.$$

From (1.20), $i = n - 2$, we obtain

$$a^{(n-1)} = (d^{-1}a_1^{(0)}, d^{-1}a_2^{(0)}, \ldots, d^{-1}a_{n-1}^{(0)}),$$

$$b^{(n-1)} = (t_1, t_2, \ldots, t_{n-1}).$$

Hence, taking into account (1.11), and by definition of the ZA

(1.21) $$a^{(n)} = (a_1^{(0)}, a_2^{(0)}, \ldots, a_{n-1}^{(0)}) = a^{(0)}$$

which proves theorem 1 for $d \neq 1$. For $d = 1$ it follows from (1.16).

2. A THEOREM ABOUT UNITS

To solve the title problem we shall prove

THEOREM 2. *Let the components* $a_i(w)$ *of the vector* $a^{(0)}$ *from* (1.3) *be polynomials with integer coefficients from* A. *If the* ZA *of* $a^{(0)}$ *is purely periodic with length of the primitive period* m, *and if the* $A_i^{(v)}$, *derived from this* ZA, *are also integers from* A, *then*

(2.1) $$\prod_{i=0}^{m-1} a_{n-1}^{(i)} = A_0^{(m)} + \sum_{j=1}^{n-1} a_j^{(0)} A_0^{(m+j)}$$

is a unit in a proper algebraic field.

Proof. From (1.9) we obtain $\prod_{i=1}^{m} a_{n-1}^{(i)} = A_0^{(m)} + \sum_{j=1}^{n-1} a_j^{(m)} A_0^{(m+j)}$, and, since the ZA of $a^{(0)}$ is purely periodic and $a_{n-1}^{(m)} = a_{n-1}^{(0)}$, $a_j^{(m)} = a_j^{(0)}$, $j = 1, \ldots, n-1$, we have

(2.2) $$\prod_{i=0}^{n-1} a_{n-1}^{(i)} = A_0^{(m)} + \sum_{j=1}^{n-1} a_j^{(0)} A_0^{(m+j)}.$$

The right side of (2.2) is an algebraic integer, in view of the hypothesis of theorem 2. In view of (1.10), the entries of the determinant, appearing on the left side of (1.10) are also algebraic integers, hence the inverse of $A_0^{(m)} + \sum_{j=1}^{n-1} a_j^{(0)} A_0^{(m+j)}$ is also an integer which proves theorem 2.

One may ask whether the restriction of theorem 2, that the ZA of $a^{(0)}$ must be purely periodic, is not too rigid. But we must keep in mind that if the ZA of $a^{(0)}$ is altogether periodic, then it can be made purely periodic of length m.

3. STATEMENT OF THE PROBLEM

In [4] Hasse and the author obtained the following results: Let

$$F(x) = \prod_{i=1}^{n} (x - d_i) - d; \; n \geq 2; \; d_i, d \in \mathbb{Z}. \qquad (i = 1, \ldots, n)$$

(3.1) $$d \geq 1; \; d_1 > d_2 > \ldots > d_n; \; d_1 \equiv d_i \pmod{d} \qquad (i = 2, \ldots, n)$$

$$d_1 - d_i \geq nd \qquad (i = 2, \ldots, n).$$

For $d = 1$ and $n = 3,4$ there are further restrictions.

Then the following statements are true:

(3.2) F(x) has exactly n different real roots;

(3.3) F(x) is irreducible over Q;

(3.4) If w is the largest root of F(x) ($d_1 < w < d_1 + 1$), then, choosing n different proper vectors $a^{(0)}$ in Q(w), the Modified Jacobi-Perron Algorithm for each of these vectors becomes purely periodic with length of primitive period $m = n(n-1)$.

(3.5) The numbers $e_i = d^{-1}(w - d_i)^n$, $(i = 1, \ldots, n-1)$ form a maximal independent system of units in Q(w).

Of course, one derives from (3.1), (3.4) and (3.5) that $e_n = d^{-1}(w - d_n)^n$ is also a unit in Q(w), and that

(3.6) $$\prod_{i=1}^{n} e_i = 1.$$

Since $e_i e_j^{-1}$ is also a unit, it follows that $((w - d_i)(w - d_j)^{-1})^n$ is a unit, hence

(3.7) $$g_i = (w - d_1)^{-1}(w - d_i), \qquad (i = 2, \ldots, n-1), \quad \text{and } e_1$$

form also a complete system of independent units in Q(w). If $d = 1$, then in (3.5) the exponent n has to be replaced by 1. Halter-Koch generalized in [3] the polynomial (3.1) in the following way:

Let f(x) be an irreducible monic polynomial with coefficients in $\mathbb{Z}$ such that

$$f(x) = \prod_{d=1}^{r_1} (x - d_j) \prod_{j=r_1+1}^{r_1+r_2} (x - z_j)(x - \bar{z}_j) - d \quad \text{with}$$

(3.1a) $$r_1 \geq 0, \; r_2 \geq 0, \; n = r_1 + 2r_2 \geq 3; \; d, d_j \in \mathbb{Z}, \; d \neq 0; \; d_1 > d_2 > \ldots > d_{r_1},$$

(3.8) z_j are integral, complex quadratic, $\bar{z}_j$ their conjugates,

$$d|d_i - d_j,\ d|d_i - z_j,\ d|z_i - z_j,\ d|z_i - \bar{z}_j,$$

for all possible indices i,j; if $r_1 = 3$, $r_2 = 0$, $|d| = 2$, then additionally $d_1 - d_2 \geq 4$ or $d_2 - d_3 \geq 4$.

On the basis of (3.8), Halter-Koch proves that f(x) has exactly r_1 (different) real zeros and exactly r_2 (different) pairs of complex conjugate zeros. To prove this, he needs the additional restrictions:

(3.9) $|d_i - d_j|,\ |d_i - z_j|,\ |z_i - z_j|,\ |z_i - \bar{z}_j| \geq 2,$ for all possible indices i,j.

In Q(w), f(w) = 0, a complete system of fundamental units consists of $r_1 + r_2 - 1$ elements. Halter-Koch proves that for $|d| > 1$

$$(3.10)\qquad e_i = \begin{cases} d(w - d_i)^{-n}, & 1 \leq i \leq r_1 \\ d^2((w - z_i)(w - \bar{z}_i))^{-n}, & r_1 + 1 \leq i \leq r_1 + r_2 \end{cases}$$

are $r_1 + r_2$ units in Q(w) with $\prod_{j=1}^{r_1+r_2} e_j = 1$, and that any (different) $r_1 + r_2 - 1$ of them form a complete system of independent units in Q(w). For $|d| = 1$, the exponent n in (3.10) has to be replaced by 1.

4. THE SOLUTION OF THE PROBLEM

We introduce the notation

$$(4.1)\qquad \{D_1, D_2, \ldots, D_n\} = \{d_1, d_2, \ldots, d_{r_1}, z_{r+1}, \bar{z}_{r+1}, \ldots, z_{r_1+r_2}, \bar{z}_{r_1+r_2}\}$$

where d_i, z_j, $\bar{z}_j$ ($i = 1, \ldots, r_1$; $z_j, \bar{z}_j = r_1 + 1, \ldots, r_1 + r_2$) are given by (3.1a), and rewrite f(x) from (3.1a) as follows:

$$(4.2)\qquad f(x) = (x - D_1)(x - D_2) \ldots (x - D_n) - d.$$

Rearranging f(x), we obtain

$$(4.3)\quad f(x) = (x - D_1)[(x - D_1) + (D_1 - D_2)] \ldots [(x - D_1) + (D_1 - D_n)] - d;$$

denoting

(4.4) $w - D_1 = \alpha$; S_i are the elementary symmetric functions in $D_1 - D_i$ ($i = 2, \ldots, n$),

we obtain from (4.3), (4.4), with f(w) = 0,

$$(4.5)\qquad f(w) = \alpha^n + S_2\alpha^{n-1} + \ldots + S_n\alpha - d = 0; \qquad w = D_1 + \alpha$$

since, by (3.8), $d|D_1 - D_i$, we have

$$(4.6)\qquad d|S_i, \quad (i = 2, \ldots, n).$$

Hence we can apply theorem 1 to the vector

$$(4.7)\qquad \begin{aligned} a^{(0)} &= (\alpha + S_2, \alpha^2 + S_2\alpha + S_3, \ldots, \alpha^{n-1} + S_2\alpha^{n-2} + \ldots + S_n) \\ a^{(0)}_{n-1} &= d\alpha^{-1}; a^{(i)}_{n-1} = \alpha^{-1} \qquad (i = 1,2, \ldots, n-1). \end{aligned}$$

In virtue of theorem 2 a unit in $Q(\alpha)$ is therefore given by

$$(4.8)\qquad \ell = d\alpha^{-n} = d(w - D_1)^{-n}.$$

If $D_1 \in \{d_1, d_2, \ldots, d_{r_1}\}$, we obtain from (4.8) the Halter-Koch units

$$(4.9)\qquad \ell_i = d(w - d_i)^{-n}, \qquad (i = 1, \ldots, r_1); \qquad \ell_i \in Q(w).$$

Otherwise we take the unit

$$(4.10)\qquad \ell_j = d(w - z_j)^{-n} \cdot d(w - \bar{z}_j)^{-n}, \qquad (j = r_1 + 1, \ldots, r_1 + r_2)$$

to obtain the other Halter-Koch units in order to construct a complete maximal set of independent units in $Q(w)$. The reader should note that

$$(4.11)\qquad \ell_j = d^2 [w^2 - (z_j + \bar{z}_j)w + z_j\bar{z}_j]^{-n} \in Q(w).$$

REFERENCES

1. Bernstein, L. *The Jacobi-Perron algorithm—Its theory and application.* Lecture Notes in Mathematics, 207. Springer-Verlag, Berlin-New York, 1971.

2. ———, *The modified algorithm of Jacobi-Perron.* Mem. Amer. Math. Soc. No. 67 (1966), 1–44.

3. ———, *Der Hasse-Bernsteinsche Einheitensatz fuer den verallgemeinerten Jacobi-Perronschen Algorithmus.* Abh. Math. Sem. Univ. Hamburg 43 (1975), 192–202.

4. Bernstein, L. and Hasse, H. *An explicit formula for the units of an algebraic number field of degree $n \geq 2$.* Pacific J. Math. 30 (1969), 293–365.

5. ———, *Einheitenberechnung mittels des Jacobi-Perronschen Algorithmus.* J. Reine Angew. Math. 218 (1965), 51–69.

6. Halter-Koch, F. *Unabhaengige Einheitensysteme fuer eine allgemeine Klasse algebraischer Zahlkoerper.* Abh. Math. Sem. Univ. Hamburg 43 (1975), 85–91.

7. Jacobi, C.G.J. *Allgemeine Theorie der kettenbruchaehnlichen Algorithmen, etc.* J. Reine Angew. Math. 69 (1869), 29–64.

8. Perron, O. *Grundlagen füer eine Theorie des Jacobischen Kettenbruchalgorithmus.* Math. Ann. 64 (1907), 1–76.

9. Stender, H.-J. *Einheiten füer eine allgemeine Klasse algebraischer Zahlkoerper.* J. Reine Angew. Math. 257 (1972), 151–178.

Department of Mathematics,
Illinois Institute of Technology,
Chicago, Illinois, 60616