An Algorithm for Field Operations on Algebraic Numbers

J. O. Shallit
University of California, Berkeley

Written around 1979

Abstract

This note describes an algorithm for computing the coefficients of a polynomial having $\alpha + \omega$ (or $\alpha - \omega$, $\alpha \cdot \omega$ or α/ω) as a root, given the coefficients of polynomials f, g such that $f(\alpha) = g(\omega) = 0$. If $\deg f = m$, $\deg g = n$, the algorithm requires $O(m^4 n^4)$ (possibly multiprecise) integer operations.

Let α be a root of $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0$ and ω be a root of $g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$, where $a_i, b_j \in \mathbb{Z}$. Thus α and ω are algebraic integers. First we compute polynomials for the sum, difference, and product of the roots, postponing quotient, as well as the case where f and g are not monic.

We now show how to compute certain matrices of integers related to α and ω. Suppose R is a finitely generated integral domain with field of fractions K. If $x \in K$ and $\sigma R \subseteq R$ and $x_1, \ldots, x_k$ generates R over $\mathbb{Z}$ then

$$\sigma \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_k \end{pmatrix} = M(\sigma) \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_k \end{pmatrix}$$

for some k by k matrix $M(\sigma)$ with entries in $\mathbb{Z}$. (Note: M is not necessarily unique.) Then

$$(\sigma I_k - M(\sigma)) \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_k \end{pmatrix} = 0$$

where I_k is the k by k identity matrix. Hence

$$\det(\sigma I_k \; - \; M(\sigma)) \; = \; 0$$

and so σ is a root of the characteristic polynomial for the matrix $M(\sigma)$, which we denote by $p_\sigma(x)$. It can be computed from $M(\sigma)$ in $O(k^4)$ steps by Frame's algorithm [1,2]. This algorithm uses only integer operations.

Now the ring $\mathbb{Z}[\alpha]$ is generated by

$$1 \; , \; \alpha \; , \; \alpha^2 \; , \; \ldots \; , \; \alpha^{m-1}$$

and in a similar fashion, the ring $\mathbb{Z}[\omega]$ is generated by

$$1 \; , \; \omega \; , \; \omega^2 \; , \; \ldots \; , \; \omega^{n-1}.$$

Therefore the ring $\mathbb{Z}[\alpha, \omega]$ is generated by the mn products $a^i\omega^j$, $0 \le i \le m-1 \; , \; 0 \le j \le n-1$.

If we order these products and define

$$\mathbf{v} \; = \; (x_1, \; x_2, \; \ldots, \; x_k)$$

$$= \; (1, \; \omega, \; \ldots, \; \omega^{n-1}, \; \alpha, \; \alpha\omega, \; \ldots, \; \alpha\omega^{n-1}, \; \ldots, \; \alpha^{m-1}, \; \alpha^{m-1}\omega, \; \ldots, \; \alpha^{m-1}\omega^{n-1})$$

then the matrix $M(\alpha)$ such that $\alpha\mathbf{v} \; = \; M(\alpha) \cdot \mathbf{v}$ has an especially simple form:

$$M(\alpha) \; = \; \begin{bmatrix} 0 & \begin{bmatrix} & \\ & I_{n(m-1)} \end{bmatrix} \\ [-a_0 I_n] \; [-a_1 I_n] & \cdots \; [-a_{m-1} I_n] \end{bmatrix}$$

We can form $M(\alpha)$ in $O(m^2n^2)$ operations.

If we now choose a new ordered set of generators

$$\mathbf{v}' \; = \; (x'_1, \; \ldots, \; x'_k)$$

$$= \; (1, \; \alpha, \; \ldots, \; \alpha^{m-1}, \; \omega, \; \alpha\omega, \; \ldots \alpha^{m-1}\omega, \; \ldots, \; \omega^{n-1}, \; \alpha\omega^{n-1}, \; \ldots, \; \alpha^{m-1}\omega^{n-1})$$

then the matrix $M'(\omega)$ for

$$\omega \begin{pmatrix} x'_1 \\ x'_2 \\ \cdot \\ \cdot \\ \cdot \\ x'_k \end{pmatrix}$$

has a similar form. We would like to perform operations on $M(\alpha)$ and $M'(\omega)$; but $M'(\omega)$ is paired with $\mathbf{v}'$ and $M(\alpha)$ is paired with $\mathbf{v}$. By reordering the rows and columns of $M'(\omega)$, however, we can get a new matrix $M(\omega)$ compatible with $M(\alpha)$.

In fact, if

$$\pi \;=\; \begin{pmatrix} 1 & 2 & 3 & \cdots & n & n+1 & \cdots & mn \\ 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 & 2 & \cdots & mn \end{pmatrix}$$

then $\mathbf{v}'_i \;=\; \mathbf{v}_{\pi i}$ and so $M'_{\pi i, \pi j}(\omega)$ is also paired with $\mathbf{v}$. We can form $M(\omega)$ in $O(m^2 n^2)$ operations.

Now

$$\begin{aligned}(\alpha+\omega)\mathbf{v} \;&=\; \alpha\mathbf{v} + \omega\mathbf{v} \\ &=\; M(\alpha)\cdot\mathbf{v} + M(\omega)\cdot\mathbf{v} \\ &=\; (M(\alpha)+M(\omega))\cdot\mathbf{v}\end{aligned}$$

and similarly

$$\begin{aligned}\alpha\omega\mathbf{v} \;&=\; \alpha M(\omega)\cdot\mathbf{v} \\ &=\; M(\alpha)M(\omega)\cdot\mathbf{v}.\end{aligned}$$

Thus, for example, $\det((\alpha+\omega)I_k - (M(\alpha)+M(\omega)) \;=\; 0$ gives a monic polynomial with $\alpha+\omega$ as a root. This is the same as performing Frame's algorithm on $M(\alpha)+M(\omega)$. The total operation count is $O(m^4 n^4)$ integer operations. The coefficients of the resulting polynomial get large quickly, but this is an inherent feature of the problem, since the resulting polynomial will almost always be irreducible.

In a similar fashion, the characteristic polynomial for $M(\alpha)M(\omega)$ will have $\alpha\omega$ as a root. Since if $p\,\in\mathbb{Z}$ then $p\omega\mathbf{v} \;=\; pM(\omega)\mathbf{v}$, we see that the characteristic polynomial for $pM(\omega)$ has $p\omega$ as a root. In particular, for $p \;=\; -1$ this gives the fact that the characteristic polynomial for $M(\alpha) - M(\omega)$ has $\alpha-\omega$ as a root. This solves the problem for sum, difference, and product.

It is easy to convert the case where f and g are not monic to the problem treated above. We do this for $\alpha+\omega$, the other cases being treated in a similar fashion.

Suppose $f(x) \;=\; a_m x^m + \cdots + a_0$, $g(x) \;=\; b_n x^n + \cdots + b_0$. Then $a_m^{m-1} b_n^m f(x) \;=\; f_1(a_m b_n x)$, $a_m^n b_n^{n-1} g(x) \;=\; g_1(a_m b_n x)$, where f_1 and g_1 are monic polynomials in $a_m b_n x$. Applying the procedure described above, we find a monic polynomial $p(x)$ with $a_m b_n(\alpha+\omega)$ as a root. Then $(a_m b_n)^{mn} p(\frac{x}{a_m b_n})$ is a polynomial with integer co-efficients with $\alpha+\omega$ as a root.

It remains to determine the polynomial for α/ω. This can be done if the constant term b_0 is non-zero (otherwise remove powers of x). The method is to observe that if ω is a root of

$$g(x) \;=\; b_n x^n + \cdots + b_0 \;=\; 0$$

then ω^{-1} is a root of

$$g_2(x) \;=\; x^n g(1/x) \;=\; b_0 x^n + \cdots + b_n \;=\; 0.$$

Hence we simply reverse the coefficients of g before performing the multiplication algorithm.

The author has implemented the above algorithm in APL, and has used the results to form inputs to a continued fraction algorithm for real roots of polynomials [3].

References

1. D. K. Faddeev and V. N. Faddeeva, *Computational Methods of Linear Algebra, W. H. Freeman*, San Francisco, 1963.

2. T. A. Bickart, APL Program for Frame's Algorithm, *APL Quote-Quad*, No. 4 (January, 1970).

3. D. Rosen and J. Shallit, A Continued Fraction Algorithm for Approximating All Real Polynomial Roots, *Mathematics Magazine* **51** (1978), 112–116.