SOME ITERATIONS FOR FACTORING A POLYNOMIAL II

A GENERALIZATION OF THE SECANT METHOD

G. W. Stewart
Departments of Mathematics
and Computer Sciences
Carnegie-Mellon University

February, 1973

This work was supported in part by the Office of Naval Research under Contract No. N00014-67-A-0314-0018.

ABSTRACT

This paper describes an iterative method for factoring a polynomial that bears the same relation to Bairstow's method as the secant method in a single variable bears to Newton's method. Like the secant method, the generalized secant method requires only one function evaluation for each iteration, and like the secant method it converges to a simple factor with order $(1+\sqrt{5})/2$.

This note is an addendum to an earlier paper by the author [4]. For the convenience of the reader we shall begin with a brief summary of the notion and results of that paper.

Let f be a monic polynomial of degree n having complementary relatively prime, monic factors u and v of degrees m and n-m. Let p and q be monic approximation to u and v. We seek correction d and e of degrees m-1 and n-m-1 so that $p^* = p+d$ and $q^* = q+e$ are better approximations to u and v. Samelson's method [1,3] determines such corrections by dropping second order terms in the equation

$$(p+d)(q+e) = f$$

to obtain

$$pd + qe = f-pq. \tag{1}$$

Equation (1) determines a system of linear equations for the coefficients of d and e. However, the system is of order n-2, and its solution by ordinary methods is prohibitively expensive for the application at hand. This difficulty can be circumvented as follows. Let

$$p(z) = b_0+b_1z+\dots+z^m,$$

and let

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -b_0 \\ 1 & 0 & \dots & 0 & -b_1 \\ 0 & 1 & \dots & 0 & -b_2 \\ \vdots & & & \vdots & \\ 0 & 0 & \dots & 1 & -b_{m-1} \end{pmatrix}$$

be the <u>companion matrix</u> whose eigenvalues are the zeros of p. Then it is shown in [4] that if h is rational and $h(F_p)$ is defined, the first column of $h(F_p)$ is the vector of coefficients of the polynomial interpolating h at the zeros of p. In particular, since d is of degree m-1, the first column of $d(F_p)$ is the vector of coefficients of d itself. Since $p(F_p) = 0$, it follows from (1) that

$$q(F_p)\tilde{d} = f(F_p)e_1, \tag{2}$$

where $\tilde{d}$ denotes the vector of coefficients of d and $e_1 = (1,0,\ldots,0)^T$. If p and q are relatively prime, then $q(F_p)$ is nonsingular. Moreover, if p is small (in the most immediate application, finding quadratic factors of a real polynomial, p is two), then the system (2) can be solved inexpensively.

Of course the process can be iterated by replacing p by p*. Depending on the choice of the complementary approximation q*, different iterations are obtained. Samelson's iteration takes q* = q+e, where e satisfies (1). This iteration converges quadratically to a simple factor. A generalization of an iteration of Jenkins and Traub [2], takes q* to be the result of applying Samelson's method to p* and q. This method converges with order about 2.62. A generalization of Bairstow's method takes q* to be the quotient obtained by dividing f by p*, and like Bairstow's method the iteration converges quadratically.

The iteration of this note is obtained as follows. With a slight change in notation, let p_0 and p_1 be initial approximations to u. Let q_1 be the quotient of f and p_0. Then p_2 is taken to be the approximate factor obtained by applying Samelson's method to p_1 and q_1.

To see that this method is a generalization of the secant method, let

$$p_{i+1} = p_i + d_i \qquad (i = 1,2).$$

If the equation

$$p_0 q_1 + r_0 = f$$

is evaluated at F_{p_1}, the result is

(3) $$p_0(F_{p_1})q_1(F_{p_1}) = f_0(F_{p_1}) - r_0(F_{p_1}).$$

From (2), (3) and the fact that $p_0(F_{p_1}) = -d_0(F_{p_1})$ we get

(4) $$[r_0(F_{p_1}) - f(F_{p_1})]\tilde{d}_1 = d_0(F_{p_1})f(F_{p_1})e_1.$$

When m=1, this reduces to the secant method for correcting the single zero of p_1.

The method may of course be applied iteratively, generating a sequence of approximate factors $p_0, p_1, p_2, \ldots$ The calculation of p_{k+1} requires the evaluation of $r_{k-1}(F_{p_k})$ and $f(F_{p_k})$. The first quantity may be obtained from the vector $\tilde{r}_{k-1} = f(F_{p_{k-1}})e_1$, which was evaluated at the previous iteration. Thus, like its prototype, the generalized secant method required only one function evaluation for each iteration.

If m is small, the solution of the system (4) will not be prohibitively expensive. However, it may happen that the matrix $r_0(F_{p_1}) - f(F_{p_1})$ is singular. It should be noted that this does not mean that the iteration is not well defined. As long as p_0 and p_1 are sufficiently near u, the quotient q_1 will be near enough v so that $q_1(F_{p_1})$ is nonsingular, and this is all that is needed for the existence of p_2. We shall return to the problem of the singularity of $r_0(F_{p_1}) - f(F_{p_1})$ at the end of this note.

The machinery developed in [4] makes the analysis of the generalized secant method easy. Let

$$\mu_i = u - p_i$$

and

$$\nu_i = v - q_i$$

be the errors in p_i and q_i. Let $\|\cdot\|$ denote the vector 1- norm and the subordinate matrix column sum norm. Then if p_0 is sufficiently near u, $p_0(F_v)$ is nonsingular. Moreover from equation (4.6) of [4],

$$(5) \qquad \|\tilde{\nu}_1\| \le \|p_0(F_v)^{-1}\| \, \|v(F_{p_0})\| \, \|F_v\|^{m-1} \|\tilde{\mu}_0\| \, .$$

Thus as p_0 approaches u, q approaches v, and for p_1 sufficiently near u the matrix $q_1(F_{p_1})$ is nonsingular, which guarantees the existence of p_2. Also from equation (3.6) of [4],

$$(6) \qquad \|\tilde{\mu}_2\| \le \|q_1(F_{p_1})^{-1}\| \, \|F_{p_1}\|^{n-m-1} \|\tilde{\mu}_1\| \, \|\tilde{\nu}_1\| \, .$$

Combining (5) and (6), we obtain the following Lemma.

<u>Lemma</u>. For all p_0 and p_1 sufficiently near u, the generalized secant approximate is well defined and satisfies

$$\|\tilde{\mu}_2\| \le S(\tilde{\mu}_1, \tilde{\mu}_0) \|\tilde{\mu}_1\| \, \|\tilde{\mu}_0\| \, ,$$

where

$$S(\tilde{\mu}_1, \tilde{\mu}_0) = \|p_0(F_v)^{-1}\| \, \|q_1(F_{p_1})^{-1}\| \, \|v(F_{p_0})\| \, \|F_v\|^{m-1} \|F_{p_1}\|^{n-m-1}$$

Since S is a continuous function of $\tilde{\mu}_1$ and $\tilde{\mu}_0$, there is a neighborhood $\mathcal{U}$ of u for which S is bounded by a constant, say $\bar{S}$. If $p_0, p_1 \in \mathcal{U}$ are sufficiently small, then all subsequent iterates belong to $\mathcal{S}$ and their errors are bounded by the corresponding solutions of the difference equation

$$\epsilon_{i+1} = \bar{S}\epsilon_i\epsilon_{i-1},$$

where

$$\epsilon_0 = \|\tilde{\mu}_0\|,\ \epsilon_1 = \|\tilde{\mu}_1\| .$$

As is well known, if ϵ_0 and ϵ_1 are sufficiently small, the ϵ_i converge to zero with order $(1+\sqrt{5})/2$. This proves the following theorem.

Theorem. There is a neighborhood $\mathcal{U}$ of u such that whenever p_0 and p_1 belong to U, the generalized secant iteration converges to u with order at least $(1+\sqrt{5})/2 \cong 1.62$.

In practice the iteration is preferable to Samuelson's or Bairstow's method only if the explicit computation of q_1 can be avoided, which requires that we use equation (4) to determine the corrections $\tilde{d}_i$. Since we never expect $q_i(F_{p_i})$ to be singular, it follows that the singularity of the matrix $r_{i-1}(F_{p_i}) - f(F_{p_i})$ is equivalent of the singularity of the matrix $p_{i-1}(F_{p_i})$, which can occur only when p_{i-1} and p_i have common zeros. This of course can happen if p_0 and p_1 are unfortunately chosen. It can also happen if at some stage the iteration produces an approximate factor with one zero far more accurate than the others; for that zero will remain undisturbed in subsequent iterations, in effect a common zero. However, in the most important application, where m=2, such partial convergence can be easily detected and the offending zero removed.

REFERENCES

1. Householder, A. S. and Stewart, G. W.: Comments on "Some iterations for factoring a polynomial." Numer. Math. 13 (1969) 470-471.

2. Jenkins, M. A. and Traub, J. F.: A three-stage variable-shift iteration for polynomial zeros and its relation to generalized Rayleigh iteration.

3. Samelson, Klaus: Faktorisierung von Polynomen durch funktionale Iteration. Bayer. Akad. Wiss. Math. Nat. Kl. Abh. 95 (1958).

4. Stewart, G. W.: Some iterations for factoring a polynomial. Numer. Math. 13 (1969) 458-470.