FAST ALGORITHMS FOR SOLVINGTOEPLITZ SYSTEM OFEQUATIONS AND FINDING RATIONALHERM-ITE INTERPOLANTS

by

David Y. Y. Yun

STAN-CS-79-748
July1979

DEPARTMENT OF COMPUTER SCIENCE
School of Humanities and Sciences
STANFORD UNIVERSITY

FAST ALGORITHMS FOR SOLVING TOEPLITZ SYSTEMS OF EQUATIONS AND FINDING RATIONAL HERMITE INTERPOLANTS

David Y. Y. Yun

Computer Science Department
Stanford University
Stanford, California 94305

Let $x_0, x_1, x_2, \ldots$ be a bounded sequence of points some of which may be repeated, The problem of **Rational Hermite Interpolation** of type (m,n) where $m+n=N$ is to determine a rational function $R_{mn}(x) = U(x)/V(x)$ with $\deg(U) \le m$ and $\deg(V) \le n$, which interpolates an analytic function f(x) at the first $N+1$ points of the sequence. If a point x_i is repeated $m_i + 1$ times then $R_{mn}(x)$ should interpolate f(x) and its first m_i derivatives at x_i. **Hermite** solved this problem for $(m,n) = (N,0)$ by constructing the **Hermite Interpolating Polynomial** $P_N(x)$ such that

$$f(x) - P_N(x) = g(x) \prod_{i=0}^{N} (x - x_i)$$

where g(x) is analytic. The general problem of **Rational Hermite Interpolation** is to find all R_{mn} satisfying $m + n = N$ which also interpolate f(x) i.e.,

$$f(x) - R_{mn}(x) = g(x) \prod_{i=0}^{N} (x - x_i) \qquad (1)$$

The two extreme cases for this problem have special names : When the sequence of points are distinct it is called **Cauchy Interpolation** and when all the points are the same it is called **Padé Table.**

A rational function $R_{mn}(x) = U(x)/V(x)$ is said to solve the **Modified Hermite Interpolation Problem** if

$$U(x) \equiv f(x)V(x) \bmod \prod_{i=0}^{N} (x - x_i) \qquad (2)$$

This research was supported in part by National Science Foundation grant MCS-77-23738 and by Office of Naval Research contract N00014-76-C-0330. Reproduction in whole or in part is permitted for any purpose of the United States government.

If $R_{m,n}(x)$ solves equation (1) then equation (2) is automatically satisfied. However, for some choices of m and n equation (1) may have no solutions, and in that case there is a parameterized family of solutions to equation (2). However, each solution $(U(x),V(x))$ to equation (2) then yields the same rational function. This unique function is called the $(m,n)^{th}$ **Rational Interpolant** for f(x). Thus the set of rational interpolants for f(x), which is called the **Rational Interpolation Table** for f(x), contains all solutions to the problem of rational Hermite interpolation.

D. Warner studied this problem in his thesis [12]. In [13], he showed all solutions to the Modified Hermite Interpolation Problem could be computed by Kronecker's Algorithm [8]. We have independently discovered this and the result that Padé approximants can be computed by Euclid's Algorithm prior to the paper of McEliece and Shearer [9]. Additionally, we have shown that Kronecker's Algorithm and the Extended Euclidean Algorithm are virtually the same. Our results go beyond those of [8,9] to include new computional techniques as well as theoretical unifications.

Let $U_0 = \prod_{i=0}^{N}(x-x_i)$ and $U_1 = \sum_{i=0}^{N} a_i x^i$ be the Hermite interpolation polynomial of f(x) . The extended Euclidean algorithm applied to U_0 and U_1 computes a sequence of quotients and remainders according to the formula for division:

$U_{i+1} = U_{i-1} - Q_i U_i$ together with iterations for computing the "comultipliers":

$W_{i+1} = W_{i-1} - Q_i W_i$ and $V_{i+1} = V_{i-1} - Q_i V_i$ for $i \geq 1$, where initially

$W_0 = 1,\ W_1 = 0,\ V_0 = 0,\ V_1 = 1.$

Now, an important relation holds for each i :

$$W_i U_0 + V_i U_1 = U_i ,$$

and the following results can be established for the Rational Interpolation Table.

Lemma 1: Each step of the extended Euclidean computation gives rise to a unique entry (in lowest terms) of the Rational Interpolation Table.

Lemma 2: The rational function U_i/V_i obtainable via the extended Euclidean computation yields $\deg(Q_i)$ equal entries of the Rational Interpolation Table along the $(m + n)^{th}$ anti-diagonal.

Theorem 1 (Euclid-Hermite): All entries along the $(m+n)^{th}$ anti-diagonal of the Rational Interpolation Table for the analytic function f(x) are computed uniquely by the extended Euclidean algorithm.

Lemma 1 and 2 and Theorem 1 have their Cauchy and Padé counterparts. The Padé Table is well known and has been extensively studied; see [3] for an excellent survey article. As an example we state the above results in the Padé case. Let $x_0 = x_1 = . . . = 0$, $U_0(x) = x^{N+1}$ and $U_1(x) = \sum_{i=0}^{N} a_i x^i$ be the first IV + 1 terms of the Maclaurin expansion of $f(x)$. Assuming the usual definition for the Padé Table, we have the following results:

Lemma 1P: Each step of the extended Euclidean computation gives rise to a unique entry (in lowest terms) of the Padé Table.

Lemma 2P: The rational function U_i/V_i obtainable via the extended Euclidean computation yields $\deg(Q_i)$ equal entries of the Padé Table along the $(m + n)^{th}$ anti-diagonal.

Theorem 1P (Euclid-Pad&): All entries along the $(m + n)^{th}$ anti-diagonal of the Padé Table for the Maclaurin series of f(x) are computed uniquely by the extended Euclidean algorithm.

Fast Computation of an arbitrary iterate of the Extended Euclidean Algorithm

The computational aspects of the problems of the previous section can be realized by an asymptotically fast extended Euclidean algorithm. We have improved and extended the HGCD algorithm of Aho, Hopcroft, and Ullman [1] in two significant ways. First, we have developed an improved HGCD algorithm called EMGCD (for Extended Middle *GCD*).

EMGCD produces the 2 by 3 matrix of polynomial entries

$$M_j = \begin{pmatrix} U_j & W_j & V_j \\ U_{j+1} & W_{j+1} & V_{j+1} \end{pmatrix}, \text{ where } \begin{pmatrix} U_j \\ U_{j+1} \end{pmatrix} = \begin{pmatrix} W_j & V_j \\ W_{j+1} & V_{j+1} \end{pmatrix} \begin{pmatrix} U_0 \\ U_1 \end{pmatrix}.$$

The cost of EMGCD is less than the cost of HGCD; however, both algorithms have an $O(N \log^2 N)$ asymptotic cost. Thus U_j and U_{j+1} are computed free relative to HGCD. Note also that algorithm EMGCD computes all of U, V, and W which are the essential quantities of the extended Euclidean algorithm. The second improvement comes from generalizing EMGCD. We have developed algorithm PRSDC (Polynomial Remainder Sequence by Divide and Conquer) which produces any desired iterate M_j in the PRS sequence and not just the middle term. The cost of PRSDC is also $O(N \log^2 N)$

Algorithm PRSDC has many useful applications. One example is the computation of the greatest common divisor of two polynomials A and B. By setting $U_0(x) = A(x)$ and $U_1(x) = B(x)$ and specifying $U_{k+1}(x) = 0$ or $\deg(U_k) \geq 0$ we can compute, using algorithm PRSDC

$$U_k(x) = GCD(A(x), B(x)) = W_k(x)A(x) + V_k(x)B(x) .$$

Another example of its utility concerns fast computational algorithms for the above Theorems. Using algorithm PRSDC we can compute an arbitrary entry R_{mn} where $m + n = N$ of the Rational Interpolation Table starting with $U_0 = \prod_{i=0}^{N}(x - x_i)$ and $U_1 =$ the Hermite interpolation polynomial of f(x) through these N+ 1 points. Gustavson [4] has shown, using the ideas of Yun [14], that starting with x_i, $f^{(j)}(x_i)$, $j = 0, \ldots, m_i$, $i = 1, \ldots, k$ that the Hermite Interpolation polynomial $P_N(x)$ through these k distinct points can be found in $O(N \log^2 N)$. Combining these facts we can state the foliowing

Theorem 2 (Euclid-Hermite-Cauchy-Pade): An arbitrary entry of the Rational Interpolation Table for the analytic function f(x) can be computed in $O(N \log^2 N)$ where N is the degree of the relevant Hermite interpolating polynomial.

Fast Toeplitz Computation

For the case $m = n$, equating coefficients of $x^n, x^{n+1},\ldots, x^{2n}$ in the relation for the (n,n) Padé approximant, we get a Toeplitz system:

$$\begin{pmatrix} a_n & \cdot & a_0 \\ & \cdot & \\ a_{2n} & & a_n \end{pmatrix} \begin{pmatrix} v_0 \\ \cdot \\ \cdot \\ v_n \end{pmatrix} = \begin{pmatrix} u_n \\ 0 \\ \cdot \\ 0 \end{pmatrix}$$

where the matrix, denoted by T , is Toeplitz. The vectors $u = (u_0,\ldots,u_n)^T$ and $v = (v_0,\ldots,v_n)^T$ are the coefficients of the (n,n) Padé approximant $(U_j(x),V_j(x))$. This fact and the above results suggests that Euclid's algorithm can be adapted to solve Toeplitz systems of equations. We now state a new theorem which is a compaction of two theorems due to Gohberg and Semencul [2]. This theorem reveals that the computation of v and u_n is, in fact, crucial.

Theorem 3 : Let the Toeplitz matrix

$$\tilde{T} = \begin{pmatrix} a_n & \cdot & \cdot & a_0 & a_{-1} \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot & \cdot \\ a_{2n} & & & a_n & \cdot \\ a_{2n+1} & \cdot & \cdot & \cdot & a_n \end{pmatrix}$$

be a bordering of the Toeplitz matrix T with one additional row and column consisting of all the same elements except two. Suppose $x = (x_0,\ldots,x_{n+1})^T$ and $y^R = (y_{n+1},\ldots,y_0)^T$ are solutions of $\tilde{T}x = e_0$ and $\tilde{T}y^R = e_{n+1}$ and suppose $x_0 = y_0 \neq 0$. Then T is invertible and it's inverse S is formed according to the formula

$$S = \frac{1}{x_0}\left\{\begin{pmatrix} x_0 & 0 & \cdot & 0 \\ x_1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 \\ x_n & \cdot & x_1 & x_0 \end{pmatrix}\begin{pmatrix} y_0 & y_1 & \cdot & y_n \\ 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & y_1 \\ 0 & \cdot & 0 & y_0 \end{pmatrix} - \begin{pmatrix} y_{n+1} & 0 & \cdot & 0 \\ y_n & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 \\ y_1 & \cdot & y_n & y_{n+1} \end{pmatrix}\begin{pmatrix} x_{n+1} & x_n & \cdot & x_1 \\ 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & x_n \\ 0 & \cdot & 0 & x_{n+1} \end{pmatrix}\right\} \quad (3)$$

Furthermore, suppose x and y^R solve $Tx = e_0$ and $Ty^R = e_n$ and $x_0 = y_0 \neq 0$. Then $T^{-1} = S$ is given by formula (3) with x_{n+1} and y_{n+1} set equal to zero.

The formula (3), for the system with T, was discovered by Trench [11], used by Zohar [15] and given a convolutional setting by Kailath, Viera, and Morf [7]. In [7] the formula (3) for the system with $\tilde{T}$ is shown to be the the discrete analog of the Christoffel Darboux formula. Suppose now that $\mathrm{Det}(T)\neq 0$. Ordinarily we would solve $Tx = e_0$ *to see if* $x_0 \neq 0$. If $x_0 = 0$ then formula (3) is no longer valid. However, a_{-1} and a_{2n+1} can be chosen so that $\mathrm{Det}(\tilde{T})\neq 0$. Then $x_0 = \tilde{T}_{11}^{-1} = \mathrm{Det}(T)/\mathrm{Det}(\tilde{T})\neq 0$. Thus we have the following stronger result :

Corollary 1 : For solving $Tz = b$ it is always possible to find x and y of formula (3) such that

$$x_0 = y_0 \neq 0.$$

Formula (3) is important because it expresses the inverse S as a product of Toeplitz matrices. To solve $Tz = b$ we can form four matrix-vector multiplications to affect $z = Sb$. Now we observe that the multiplication of Toeplitz matrices and the vector b given by

$$\begin{pmatrix} x_0 & 0 & \cdot & 0 \\ x_1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 \\ x_n & \cdot & x_1 & x_0 \\ x_{n+1} & x_n & \cdot & x_1 \\ 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & x_n \\ 0 & \cdot & 0 & x_{n+1} \end{pmatrix} \begin{matrix} b_0 \\ \cdot \\ \cdot \\ b_n \end{matrix} \quad \text{and} \quad \begin{pmatrix} y_{n+1} & 0 & \cdot & 0 \\ y_n & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 \\ y_1 & \cdot & y_n & y_{n+1} \\ y_0 & y_1 & \cdot & y_n \\ 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & y_1 \\ 0 & \cdot & 0 & y_0 \end{pmatrix} \begin{pmatrix} b_0 \\ \cdot \\ \cdot \\ b_n \end{pmatrix}$$

are precisely the concatenations of the four matrices in formula (3) and clearly correspond to polynomial multiplications. Performing multiplication modulo t^{n+1} via FFT with appropriate ordering of the coefficients x_i, y_i, and b_i, we can easily derive the following result :

Corollary 2 : Given x and y with $x_0 = y_0 \neq 0$, the cost of solving $Tz = b$ by effecting $z = Sb$ without explicitly computing $S = T^{-1}$ is $O(n \log n)$.

Let $U_0(x) = x^{2n+1}$ and $U_1(x) = \sum_{i=0}^{2n} a_i x^i$. The polynomial U_1 represents the Toeplitz matrix T. Now apply the extended Euclidean algorithm to U_0 and U_1. The following two theorems demonstrate the importance of this computation and establishes a direct connection between the Euclidean algorithm and the solution of Toeplitz systems of equations.

Theorem 4 : Let (U_j, V_j, W_j) be the iterate of the extended Euclidean algorithm **that** computes the (n, n) Padé approximant to U_1 . Then Det(T)#O if and **only** if $\deg(U_j) = n$.

Theorem 5 : Let (U_j, V_j, W_j) and $(U_{j+1}, V_{j+1}, W_{j+1})$ be two successive extended Euclidean iterates with $\deg(U_j) = n$. These two extended Euclidean iterates contain all the necessary information to compute x and y where $Tx = e_0$ and $Ty^R = e_n$. Furthermore, if $x_0 = 0$ then the same two extended Euclidean iterates contain all information needed to compute $\tilde{T}x = e_0$ and $\tilde{T}y^R = e_{n+1}$ with $x_0 = y_0 = 1$.

The solutions x and y can be expressed as linear combinations of the V_j and V_{j+1} polynomials. The term "all the necessary information" means that the constants of the linear combinations turn out to be natural by-products of the extended Euclidean algorithm. A partial explanation of why Theorem 5 is true is the fact that the Padé Table has many relationships (Frobenius Identities) connecting the Table entries. The condition of Theorem 5 implies that the (n, n) and $(n - 1, n + 1)$ Padé approximants are computed by successive Euclidean iterates. Theorems 4 and 5 and formula (3) provide the basis of another important application of algorithm PRSDC. We state this application as follows:

Theorem 6 (Euclid-Toeplitz) : The complexity of solving the Toeplitz system $Tz = b$ is at most $O(n \log^2 n)$ and the extended Euclidean algorithm can be used to effect the solution with this complexity.

We have also established new complexity results for banded Toeplitz systems. Let T_{bc} be a banded Toeplitz matrix whose semi-bandwidths are b and c i.e., $a_0 = \ldots = a_{n-b-1} = 0$ and $a_{n+c+1} = \ldots = a_{2n} = 0$. Then by applying PRSDC to $U_0(x) = x^{n+b+1}$ and $U_1(x) = a_{n+c}x^{b+c} + \ldots + a_{n-b}$ we can solve $Tz = d$ in $O(n \log n) + O((b + c)\log^2(b + c))$. The best previous result of $O(n \log n) + O((b+c)^2)$ is due to Jain [6] and Morf and Kailath [10, p. 269]. Theorems 4 and 5 above are valid for the banded case. The only change in their statements is the replacement of (n,n) with (b,n) and $(n-1,n + 1)$ with $(b-1,n + 1)$. Recently, Brent discovered a fast $O(n \log^2 n)$ algorithm to compute x and y via a fast continued fraction expansion. A joint paper by him and the authors is planned to detail some of the results described here. The best previous algorithm to solve Toeplitz **systems is** the $O(n^2)$ algorithm of Trench [11] corresponding to the Levinson algorithm in the **continuum.**

The Berlekamp Algorithm, Shift register synthesis, and BCH decoding

Let $S(x) = s_1 x + \ldots + s_{2n} x^{2n}$ be a given syndrome polynomial. The key equation to finding the error location polynomial of BCH decoding is

$$(1 + S(x))\sigma(x) \equiv \omega(x) \bmod (x^{2n+1})$$

where

$$a(x) = 1 + \sum_{i=1}^{e} \sigma_i x^i \text{ and } \omega(x) = 1 + \sum_{i=1}^{e} \omega_i x^i$$

and e = $\deg(\sigma) = \deg(\omega)$ is small. Berlekamp's algorithm is an $O(n^2)$ method [5] **for** computing a(x) and w(x) . Algorithm PRSDC also solves this problem. Let $U_0(x) = x^{2n+1}$ and U,(x) = 1 + S(x) . Then the iterate (U_j, V_j, W_j) of the extended Euclidean **algorithm** which computes the (n,n) Padé approximant to U_1 is the solution to the key equation. Also the complexity of this problem is lowered to $O(n \log^2 n)$.

References

[1] Aho, A. V., Hopcroft, J. E., and Ullman, J. D. *The Design and Analysis **of** Computer Algorithms,* Book, Addison Wesley, Reading, Mass., 1974

[2] Gohberg, I. C., and Semencul, A. A., "On the Inversion of Finite Toeplitz Matrices and their Continuous Analogs", Mat. Issled., 2 (1972), pp. 201-233. (In Russian) Also see Gohberg, I. C. and Feldman, 1. A., *"Convolution equations and projection methods **for** their solutions",* Translation of Math. Monographs, Vol. 41, Amer. Math. Soc., 1974.

[3] Gragg, W. B., "The Padé Table and its Relation to Certain Algorithms of Numerical Analysis", SIAM Rev., Vol. 14, No. 1, Jan. 1972, pp. l-42.

[4] Gustavson, F. G., "An $O(N \log^2 N)$ Algorithm to Compute the Hermite Interpolating Polynomial", to appear as an IBM RC Report.

[5] Gustavson, F. G., "Analysis of the Berlekamp-Massey Linear Feedback Shift-Register Synthesis Algorithm", IBM J. Res. & Dev., Vol. 20, No. 3, May 1976, pp. 204-212.

[6] Jain, A. K., "Fast Inversion of Banded Toeplitz Matrices by Circular Decompositions", IEEE Trans. on Acous., Speech, and Sig. Proc., Vol. ASSP-26, No. 2, Apr. 1978, pp. 121-126.

[7] Kailath, T., Viera, A., and Morf, M., "Inverses of Toeplitz Operators, Innovations, and Orthogonal Polynomials", SIAM Rev., Vol. 20, No. 1, Jan. 1978, pp. 106-119.

[8] Kronecker, L., "Zur Theorie der Elimination einer Variabelen aus zwei algebraisthen Gleichungen", Monatsber. Konigl. Preuss. Akad. Wiss. Berlin, 1851, pp. 535-600.

[9] McEliece, R. J. and Shearer, J. B., "A Property of Euclid's Algorithm and an Application to Padé Approximation", SIAM J. Appl. Math., Vol. 34, No. 4, June 1978, pp. 61 l-615.

[10] Morf, M. and Kailath, T., "Recent Results in Least-Square Estimation Theory", Annals of Economic and Social Measurements, 6/3/77, pp. 261-274.

[11] Trench, W. F., "An algorithm for the inversion of finite Toeplitz Matrices", J. SIAM 12, *3*, Sept. 1964, pp. 5 15-522.

[12] Warner, D. D., *Hermite Interpolation with Rational Functions*, Thesis, Univ. of Calif. at San Diego, June 11, 1974.

[13] Warner, D. D., "Kronecker's Algorithm for Hermite Interpolation with an Application to Sphere Drag in a Fluid-filled Tube". Proc. of the Workshop on Padé Approx., Feb. 1976, Eds. D. Bessis, J. Gliewicz, P. Mery, CNRS Marseilles, pp. 48-51.

[14] Yun, D. Y. Y., "Uniform Bounds for a Class of Algebraic Mappings Related to Residue Computation and Chinese Remaindering", IBM R. C. 7185, Yorktown Heights, N. Y., June 16, 1978, to appear in SIAM J. Comp., Aug. 1979.

[153 Zohar, S., "Toeplitz Matrix Inversion: The Algorithm of W. F. Trench", J. ACM 16, 4, Oct. 1969, pp. 592-601.