The Mechanization of the Comrade Matrix Approach in Determining the GCD of Orthogonal Polynomials

Siti Nor Asiah binti Isa*, **Nor'aini Aris, Shazirawati Mohd Puzi and Yeak Su Hoe**

Department of Mathematical Sciences, Faculty of Science
Universiti Teknologi Malaysia, 81310 Johor Bahru, Johor, Malaysia
*Corresponding author: snasiahisa@gmail.com

Abstract This paper revisits the comrade matrix approach in finding the greatest common divisor (GCD) of two orthogonal polynomials. The present work investigates on the applications of the QR decomposition with iterative refinement (QRIR) to solve certain systems of linear equations which is generated from the comrade matrix. Besides iterative refinement, an alternative approach of improving the conditioning behavior of the coefficient matrix by normalizing its columns is also considered. As expected the results reveal that QRIR is able to improve the solutions given by QR decomposition while the normalization of the matrix entries do improves the conditioning behavior of the coefficient matrix leading to a good approximate solutions of the GCD.

Keywords Comrade matrix; QR decomposition; refinement iteration; normalization.

Mathematics Subject Classification 33F05, 49M27.

1 Introduction

The greatest common divisor (GCD) of a polynomial set is significant to problems that arise in applied mathematics and engineering. The work mainly focuses on solving the GCD computation of two polynomials by using the theoretical approach which has been proposed in several works of Barnett [1-4]. He made use of companion and congenial matrices such as colleague, comrade and confederate matrix which can be applied to compute the GCD in the generalized form. Barnett's GCD theorem provides an alternative to standard approaches which are based on Euclidean algorithm (which has been known for centuries in GCD solving via polynomial division), since the GCD can be calculated in a single step, either symbolically or numerically, or by solving a system of linear equations.

We consider the problem of computing the GCD of two polynomials

$$
\begin{aligned}
a\left(x\right) &= a_0 p_0\left(x\right) + a_1 p_1\left(x\right) + \ldots + a_n p_n\left(x\right) \\
b\left(x\right) &= b_0 p_0\left(x\right) + b_1 p_1\left(x\right) + \ldots + b_m p_m\left(x\right)
\end{aligned}
\tag{1}
$$

with $\deg\{a(x)\} = n$ and $\deg\{b(x)\} = m$, where $n \geq m$ and $a_n, b_m \neq 0$. The polynomials coefficients are represented in a basis of orthogonal polynomials $\{p_i(x)\}_{i=0}^{n}$ defined by the three recurrence relation such that,

$$
\begin{aligned}
p_0(x) &= 1, \\
p_1(x) &= \alpha_0 x + \beta_0, \\
p_{i+1}(x) &= (\alpha_i(x) + \beta_i(x))\, p_i(x) - \gamma_i p_{i-1}(x).
\end{aligned}
\tag{2}
$$

for $i = 1, 2, 3, \cdots, n-1$ with $\alpha_i > 0$, $\beta_i > 0$, $\gamma_i > 0$. Without loss of generality, let $a_n = 1$ and $m < n$. If the values of α_i, β_i, γ_i for $i = 0, 1, \ldots, n-1$ are known, the comrade matrix for $a(x)$ is an $n \times n$ matrix given by

$$
\begin{bmatrix}
\dfrac{-\beta_0}{\alpha_0} & \dfrac{1}{\alpha_0} & \cdots & 0 & \cdots & \cdots & \cdots & 0 \\[2mm]
\dfrac{\gamma_0}{\alpha_1} & \dfrac{-\beta_1}{\alpha_1} & \dfrac{1}{\alpha_1} & 0 & \cdots & \cdots & \cdots & 0 \\[2mm]
0 & \dfrac{\gamma_1}{\alpha_2} & \dfrac{-\beta_2}{\alpha_2} & \dfrac{1}{\alpha_2} & \cdots & \cdots & \cdots & 0 \\[2mm]
\vdots & \vdots & \vdots & \vdots & \cdots & \cdots & \cdots & \vdots \\[2mm]
0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \dfrac{1}{\alpha_{n-2}} \\[2mm]
\dfrac{-a_0}{a_n\alpha_{n-1}} & \cdots & \cdots & \cdots & \cdots & \dfrac{-a_{n-3}}{a_n\alpha_{n-1}} & \dfrac{-a_{n-2}+a_n\gamma_{n-1}}{a_n\alpha_{n-1}} & \dfrac{-a_{n-1}-a_n\beta_{n-1}}{a_n\alpha_{n-1}}
\end{bmatrix}.
\tag{3}
$$

The comrade matrix above is a generalization of the companion matrix and is associated with a polynomial expressed as a linear combination of an orthogonal basis. By applying the comrade matrix approach, the degree of the GCD of these polynomials which is equalto the rank loss of the associate coefficient matrix of certain systems of linear equations, can be determined. The coefficients of the GCD are then obtained by solving these systems with respect to some variables.Aris and Rahman [5] and Ahmad [6] have applied the theoretical and analytical results of Barnett by constructing and implementing symbolic algorithms to compute the GCDs of polynomials in the orthogonal basis, particularly the Legendre and Chebyshev polynomials. The work has applied the modular homomorphic image scheme so as to avoid multiprecision operations involving very large integers and rational numbers in the entries of the matrix. Solving the problem in exact computational environment faces the challenge of applying multiprecision operations and intermediate expression swell. On the other hand, in the floating point environment the coefficient matrix can be ill conditioned. Solving the problem numerically leads to new challenges not only for the purpose of solving the GCD problem but also to investigate on the extensiveness of applying appropriate numerical methods for solving ill-conditionedsystems of linear equations, see in [7,8].

In this paper, the numerical results from using QR Householder method to solve the GCD of two polynomials in the shifted Chebyshev basis are presented. The process of iterative refinement is implemented to reach a better approximate solution.In addition when the method fails to give a correct solution, scaling the coefficient matrix is also investigated in order to reduce the condition number of the coefficient matrix and consequently finding the desired solution.

2 General Procedure

Let $a(x)$ and $b(x)$ be two polynomials satisfying relation (2), with $\deg(a(x)) = n \geq \deg(b(x)) = m$. The method of finding the GCDs of $(a(x), b(x))$ using the comrade matrix can be outlined by the following procedure:

Step 1: Construct the comrade matrix associated with $a(x)$.

Step 2: Construct the corresponding coefficient matrix of certain system of linear equations using the recurrence relation defined in (2).

Step 3: Determine the rank of the coefficient matrix in Step 2 and solve the augmented systems of linear equations to obtain the coefficients of the GCD.

2.1 Constructing the System of Equations

If A is the comrade matrix given by (3), define

$$b(A) = b_0 I + b_1 p_1(A) + \cdots + b_m p_m(A). \tag{4}$$

The respective rows of $b(A)$ is given by $r_0 = [b_0, b_1, \ldots, b_m, \ldots, b_{n-1}]$, $r_1 = r_0 p_1(A), \ldots, r_{n-1} = r_0 p_{n-1}(A)$. Using the recurrence relation defined in (2), the rows of $b(A)$ in terms of the comrade matrix and recurrence relation such that:

$$\begin{aligned}
r_0 &= (b_0, b_1, \ldots, b_m, 0, \ldots, 0), \\
r_1 &= r_0(\alpha_0 A), \\
r_i &= r_{i-1}(\alpha_{i-1} A + \beta_{i-1} I) - \gamma_{i-1} r_{i-2},
\end{aligned} \tag{5}$$

for $i = 2, \ldots, n$ The GCD of polynomials $a(x)$ and $b(x)$, denoted by $d(x) = \gcd(a, b)$, is a polynomial with degree $\deg\{d(x)\} \leq n$ such that $\deg\{\gcd(a, b)\} = n - \operatorname{rank}[b(A)]$ such that

$$d(x) = d_0 p_0(x) + d_1 p_1(x) + \cdots + p_k(x). \tag{6}$$

Theorem 1 [4] *If $c_1, c_2, \ldots, c_n$ are the columns of the coefficient matrix $b(A)$ with rank $n - k$, then the last $n - k$ columns, i.e. $c_{k+1}, \ldots, c_n$, are linearly independent and every column c_i for $i = 1, 2, \ldots, k$ can be written as linear combinations of $c_{k+1}, \ldots, c_n$. Then the coefficients $d_0, \ldots, d_{k-1}$ in (6) are given by*

$$c_i = d_{i-1} c_{k+1} + \sum_{k+2}^{n} x_{ij} c_j \quad i = 1, 2, \ldots, k. \tag{7}$$

The k-system of equations in (7) is described by the augmented matrix

$$\left(\begin{array}{ccccc|cccc} c_{k+1} & \vdots & c_{k+2} & \vdots & \cdots & \vdots & c_n & \| & c_1 & \vdots & \cdots & \vdots & c_k \end{array} \right) \tag{8}$$

which is

$$\begin{pmatrix} c_{1,k+1} & c_{1,k+2} & \cdots & c_{1,n} \\ c_{2,k+1} & c_{2,k+2} & \cdots & c_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ c_{n,k+1} & c_{n,k+2} & \cdots & c_{n,n} \end{pmatrix} \begin{pmatrix} x_{i,l+1} \\ x_{i,k+2} \\ \vdots \\ x_{i,n} \end{pmatrix} = \begin{pmatrix} c_{1,i} \\ c_{2,i} \\ \vdots \\ c_{n,i} \end{pmatrix} \tag{9}$$

for each $i = 1, 2, \ldots, k$ and $x_{i,k+1} = d_{i-1}$.

The computation of the rank of $b(A)$ and the coefficient of GCD, can be computed simultaneously from (9) and (10). The column of matrix $b(A)$ is rearranged to produce a new matrix so that the jth column of $b(A)$ is the $n - (j-1)^{th}$ column of the new matrix, say $L^{(0)}$ i.e:

$$l^0_{n-(j-1)} = c_j \text{ for } j = 1, 2, \ldots, n.$$

Reducing $L^{(0)}$ to upper row echelon form by s steps gives the matrix

$$L^{(s)} = \begin{pmatrix} l^{(s)}_{1,1} & l^{(s)}_{1,2} & \cdots & l^{(s)}_{1,r} & \vdots & l^{(s)}_{1,r+1} & \cdots & l^{(s)}_{1,r+k} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & l^{(s)}_{r,r} & \vdots & l^{(s)}_{r,r+1} & \cdots & l^{(s)}_{r,r+k} \\ 0 & 0 & \cdots & 0 & \vdots & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & \vdots & 0 & \cdots & 0 \end{pmatrix} \tag{10}$$

such that $r = \text{rank}\left(L^{(0)}\right)$. If $k = n - r$, the solution to the coefficient of $d(x)$ is given as follows:

$$d_{k-1} = l^{(s)}_{r,r+i}\text{Inv}\left(l^{(s)}_{r,r}\right), \qquad i = 1, 2, \ldots, k,$$
$$d_k = 1.$$

3 Mechanization of Comrade Matrix Approach

Due to the stability criterion of the QR decomposition method in solving least square problems and over-determined system of linear equations, the method is chosen to solve the GCD problem.

3.1 Standard QR

A standard method of obtaining QR factorization is via Gram-Schmidt orthogonalization. But this method is not as stable as QR via Householder reflectors [9], which we choose to focus in this work. The coefficient matrix $b(A)$ obtained in (5) can be partitioned into general least square problem $Ax = b$ once we know the rank. The procedure to the QR factorization are as followed:

1. QR factorization of A such that $A = QR$ (Householder reflectors).
2. Form $d = Q^T b$.
3. Solve $Rx = d$ via backward substitution.

3.2 QR with Iterative Refinement

For a small number of degree polynomials or small number of coefficient integers involved in the associated matrix, the method is always stable. But as the degree of polynomials increases, the method is not quite stable, thus requires iterative refinement step so that the initial solution approaches the desired solution. In iterative refinement a computed solution is corrected in

an iterative process. The solution to a linear problem is regarded as an initial approximation to the true solution of $Ax = b$. Then the process of iterative refinement can be described as follow:

1. Set $x^0 = \bar{x}$.
2. For $k = 1, 2, \ldots$, do
    i. Compute the residual vector: $r^{(k)} = b = Ax^{(k)}$.
    ii. Calculate the correction vector $c^{(k)}$ by solving the system $Ac^{(k)} = r^{(k)}$ using the same triangularization of A that is used to obtain the initial approximate value, $x^{(0)}$.
    iii. Update the solution: $x^{(k+1)} = x^{(k)} + c^{(k)}$.
    iv. Test for the convergence if $\frac{\|x^{(k+1)} - x^{(k)}\|_2}{\|x^{(k)}\|_2} < \varepsilon$, where ε is the convergence tolerance.
3. End.

3.3 Normalization

Considering the monic polynomials involved in this work, there is a large disparity in the sizes of coefficient matrix when the smallest entry of the $b(A)$ matrix is 1 while the largest entry has at least 10 digits. Such matrix is ill conditioned. To reduce the condition number of the matrix, we scale the matrix by dividing each entry of the matrix, say a_{ij} with the largest number in each ith rows. Examples are shown as Table 1.

Table 1: Condition Number Before and After Normalization

Test Problem	Condition Number	
m	Before normalization	After normalization
9	2.16E+29	2.75E+21
9	1.17E+30	8.47E+20
10	5.71E+30	3.87E+21
10	3.94E+34	1.01E+21

Note: m is the size of the coefficient matrix

4 Result and Discussion

The test polynomials relative to the shifted Chebyshev basis are generated by using C++ programming such that the roots are randomly generated integers without repetitions of roots.The results on the implementation of QR Householder (QR), QR with iterative refinement (QRIR) and QR with normalization (QRN) algorithms on some test problems using C++ programming are presented as shown in Table 1, Table 2 and Table 3. In the tables below, m is the degree of $a(x)$, n is the degree of $b(x)$, k is the degree of the GCD of $a(x)$ and $b(x)$. 'Digits' denote the maximum number of digits obtained from the largest coefficient matrix entry. For the test

problems, the number of digits that gives the largest coefficient matrix entry is taken to be between 20 and 32, while the smallest entry in the matrix is always 1, since the polynomials has to be monic. For digits to be in this range, the size of the polynomial roots and the degree of the polynomials can be divided into 3 different cases: small roots, degree of $a(x) \leq 10$; big roots, small degree of $a(x)$; and small roots, big degree of $a(x)$. Relative to the multiprecision integer entries of the coefficient matrix (since digits ≥ 10), the polynomials are considered of small degree if the degree is less than or equal to 7 and big degree if its degree is greater than or equal to 10. Here small roots range between -15 to 15 while large roots range up to 100.

Table 2: Small Roots, Degree $a(x) \leq 10$

Test Problem				Relative Error		
m	n	k	digits	QR	QRIR	QRN
9	8	5	22	3.15E−04	5.17E−07	1.72E−09
9	8	5	21	6.51E−06	6.30E−08	1.32E−10
10	9	4	23	1.12E−02	1.96E−09	1.96E−08
10	9	6	27	1.43E−06	7.34E−10	7.88E−07

In Table 2, it is shown that after some iterative refinement the calculated solutions are closer to the actual solutions, while by normalizing the coefficient matrix, QRN gives better results than implementing QR without normalization followed by iterative refinement (QRIR).

Table 3: Big Roots, Small Degree $a(x)$

Test Problem				Relative Error		
m	n	k	digits	QR	QRIR	QRN
7	6	3	30	5.19E−04	7.51E−09	5.85E−02
6	5	2	30	1.13E−03	1.23E−09	6.70E−04

It is shown in Table 3 that computations using QRIR gives better solutions compared to QRN. While in Table 4, when considering polynomials of degree greater than 10 with the maximum number of digits in the coefficient matrix entries about 32, only QRN is able to give a good approximate solution. This may be due to the truncation error in the precision involving multiplications and divisions involving big integers, during the reduction stages of the QR method.

Table 4: Small Roots, Big Degree $a\,(x)$

Test Problem				Relative Error		
m	n	k	digits	QR	QRIR	QRN
11	10	7	32	Fail to give solutions	Fail to give solutions	6.90E−07
12	11	5	30	Fail to give solutions	Fail to give solutions	1.67E−05
12	11	2	30	Fail to give solutions	Fail to give solutions	1.89E−03

5   Conclusion

The application of the QR algorithm is not trivial since the matrix involved in finding the solutions to the GCD is ill-conditioned. There exist limitations to the method such that to a certain extent the method fails to give the correct solution. In this work the problem can be overcome by the process of iterative refinement to achieve a better approximate solution or by the process of normalization of the matrix entries. Normalizing the entries reduce the disparity in the size of the matrix entries and thus possibly improves the conditioning behavior of the matrix.

Acknowledgement

References

[1] Barnett, S. Greatest common divisor of two polynomials. *Linear Algebra and its Applications.* 1970. 3(1): 7-9.

[2] Barnett, S. 1971. Greatest common divisor of several polynomials. *Mathematical Proceedings of the Cambridge Philosophical Society.* 1971. 70(2): 263-268.

[3] Barnett, S. A companion matrix analogue for orthogonal polynomials. *Linear Algebra and its Applications.* 1975. 12(3): 197-202.

[4] Barnett, S. Division of generalized polynomials using the comrade matrix. *Linear Algebra and its Applications.* 1984. 60: 159-175.

[5] Aris, N and Rahman, A. A. On the division of generalized polynomials. In *Computer Mathematics: Proceedings of the Sixth Asian Symposium (ASCM 2003), October 23-25.* Beijing, China: World Scientific. 2003. 10: 40-51.

[6] Aris, N and Ahmad, S. N. Computing the greatest common divisor of polynomials using the comrade matrix. In *Computer Mathematics: Proceedings of the Eighth Asian Symposium (ASCM 2007), December 15-17.* Singapore: Springer. 2007. 87-96.

[7] Isa, S. N., Aris, N. and Puzi, S. M. Numerical matrix methods in the computation of the greatest common divisor (GCD) of polynomials. *AIP Conference Proceedings*. 2016. (Vol. 1775, No. 1, p. 030064). AIP Publishing.

[8] Isa, S. N., Aris, N. and Taha, A. Z. Analysis and comparison of numerical algorithms for finding the GCD of certain types of polynomials in the Chebyshev basis. *Malaysian Journal of Fundamental and Applied Sciences*. 2017. 13(2): 68-71.

[9] Datta, B. N. *Numerical Linear Algebra and Applications*. Philadelphia: Society for Industrial and Applied Mathematics. 2010.