Christou, D., Karcanias, N. & Mitrouli, M. (2008). The Euclidean Division as an Iterative ERES-based Process. Paper presented at the Conference in Numerical Analysis NumAn 2008, 1 Sep 2008 - 5 Sep 2008, Kalamata, Greece.



City Research Online

Original citation: Christou, D., Karcanias, N. & Mitrouli, M. (2008). The Euclidean Division as an Iterative ERES-based Process. Paper presented at the Conference in Numerical Analysis NumAn 2008, 1 Sep 2008 - 5 Sep 2008, Kalamata, Greece.

Permanent City Research Online URL: http://openaccess.city.ac.uk/733/

Copyright & reuse

City University London has developed City Research Online so that its users may access the research outputs of City University London's staff. Copyright © and Moral Rights for this paper are retained by the individual author(s) and/ or other copyright holders. Users may download and/ or print one copy of any article(s) in City Research Online to facilitate their private study or for non-commercial research. Users may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain. All material in City Research Online is checked for eligibility for copyright before being made available in the live archive. URLs from City Research Online may be freely distributed and linked to from other web pages.

Versions of research

The version in City Research Online may differ from the final published version. Users are advised to check the Permanent City Research Online URL above for the status of the paper.

Enquiries

If you have any enquiries about any aspect of City Research Online, or if you wish to make contact with the author(s) of this paper, please email the team at <u>publications@city.ac.uk</u>.

The Euclidean Division as an Iterative ERES-based Process

Dimitrios Christou¹, Nicos Karcanias¹ and Marilena Mitrouli²

¹ Control Engineering Research Centre, School of Engineering and Mathematical Sciences, City University, Northampton Square, EC1V 0HB, London, U.K.

² Department of Mathematics, University of Athens, Panepistemiopolis 15784, Athens, Greece.

dchrist@math.uoa.gr, N.Karcanias@city.ac.uk, mmitroul@math.uoa.gr

Abstract. Considering the Euclidean Division of two real polynomials, we present an iterative process based on the ERES method to compute the remainder of the division and we represent it using a simple matrix form.

Introduction

The representation of the Euclidean algorithm process is presented using the matrix-based methodology of Extended-Row-Equivalence and Shifting operations (ERES) [3,4]. This allows the use of numerical methodologies for algebraic computation problems with the additional advantage of being able to handle uncertain coefficients and numerical errors.

We consider two real polynomials:

$$P(x) = \sum_{i=0}^{m} p_i x^i, \ p_m \neq 0 \quad \text{and} \quad Q(x) = \sum_{i=0}^{n} q_i x^i, \ q_n \neq 0, \quad m, n \in \mathbb{N} \quad (0.1)$$

with degrees $\deg\{P(x)\} = m$, $\deg\{Q(x)\} = n$ respectively, and $m \ge n$.

Definition 1. We define the set

$$\mathcal{D}_{m,n} = \left\{ (P(x), Q(x)) : P(x), Q(x) \in \mathbb{R}[x], \ m = \deg\{P(x)\} \ge \deg\{Q(x)\} = n \right\}$$

For any pair $\mathcal{D} = (P(x), Q(x)) \in \mathcal{D}_{m,n}$, we define a vector representative $\underline{D}(x)$ and a basis matrix D_m represented as :

$$\underline{D}(x) = [P(x), Q(x)]^t = [\underline{p}, \underline{q}]^t \cdot \underline{e}_m(x) = D_m \cdot \underline{e}_m(x)$$

where $D_m \in \mathbb{R}^{2 \times (m+1)}$, $\underline{e}_m(x) = [x^m, x^{m-1}, \dots, x, 1]^t$. The matrix D_m is formed directly from the coefficients of the given polynomials P(x) and Q(x).

Definition 2. Given a pair $\mathcal{D}_{m,n}$ of real polynomials with a basis matrix D_m the following operations are defined [3, 4]:

- a) Elementary row operations with scalars from \mathbb{R} on D_m .
- b) Addition or elimination of zero rows on D_m .
- c) If $\underline{a}^t = [0, \dots, 0, a_l, \dots, a_k] \in \mathbb{R}^k$, $a_l \neq 0$ then we define as the Shifting operation

 $shf: shf(\underline{a}^t) = [a_1, \dots, a_k, 0, \dots, 0] \in \mathbb{R}^k$

By $\operatorname{shf}(\mathcal{D}_{m,n}) \equiv \mathcal{D}_{m,n}^*$, we shall denote the pair obtained from $\mathcal{D}_{m,n}$ by applying shifting on the rows of D_m . Type (a), (b) and (c) operations are referred to as Extended-Row-Equivalence and Shifting (*ERES*) operations.

The following theorem shows the relation between a matrix and its shifted form [1].

Theorem 1 (Matrix representation of Shifting). If $D \in \mathbb{R}^{2 \times k}$, k > 2, is an upper trapezoidal matrix with rank $\rho(D) = 2$ and $D^* \in \mathbb{R}^{2 \times k}$ is the matrix obtained from D by applying shifting on its rows, then there exists a matrix $S \in \mathbb{R}^{k \times k}$ such that: $D^* = D \cdot S$.

Corollary 1. If $D_m \in \mathbb{R}^{2 \times (m+1)}$ is the basis matrix of a pair of real polynomials $\mathcal{D} = (P(x), Q(x)) \in \mathcal{D}_{m,n}$, then $D_m^* \in \mathbb{R}^{2 \times (m+1)}$ is the basis matrix of the pair $\mathcal{D}^* = (P(x), x^{m-n} Q(x)) \in \mathcal{D}_{m,m}$ and there exists a matrix $S_{\mathcal{D}} \in \mathbb{R}^{(m+1) \times (m+1)}$ such that:

$$D_m^* = D_m \cdot S_\mathcal{D} \tag{0.2}$$

The ERES representation of the Euclidean Division

If we have a pair of polynomials $\mathcal{D} = (P(x), Q(x)) \in \mathcal{D}_{m,n}$, then, according to Euclid's division algorithm, it holds:

$$P(x) = \frac{p_m}{q_n} x^{m-n} Q(x) + R_1(x)$$
(0.3)

This is the first and basic step of the Euclidean Division algorithm. The polynomial $R_1(x) \in \mathbb{R}[x]$ is given by:

$$R_1(x) = \sum_{i=m-n}^{m-1} \left(p_i - \frac{p_m}{q_n} q_{i-(m-n)} \right) x^i + \sum_{i=0}^{m-n-1} p_i x^i \tag{0.4}$$

In the following, we will show that the remainder $R_1(x)$ can be computed by applying ERES operations to the basis matrix D_m of the pair \mathcal{D} .

Proposition 1 (Matrix representation of the first remainder of the Euclidean Division). Applying the algorithm of the Euclidean Division to a pair $\mathcal{D} = (P(x), Q(x)) \in \mathcal{D}_{m,n}$ of real polynomials, there exists a polynomial $R_1(x) \in \mathbb{R}[x]$ with degree $0 \leq deg\{R_1(x)\} < m$ such that:

$$P(x) = \frac{p_m}{q_n} x^{m-n} Q(x) + R_1(x)$$

70 Dimitrios Christou, Nicos Karcanias and Marilena Mitrouli

Then, the remainder $R_1(x)$ can be represented in matrix form as:

$$R_1(x) = \underline{v}^t \cdot E_1 \cdot \underline{e}_m(x)$$

where $E_1 \in \mathbb{R}^{2 \times (m+1)}$ is the matrix, which occurs from the application of the ERES operations on the basis matrix D_m of the pair \mathcal{D} and $\underline{v} = [0, 1]^t$.

Proof. If we consider the division P(x)/Q(x), then, according to Euclid's algorithm, there is a polynomial $R_1(x)$ with degree $0 \leq deg\{R_1(x)\} < m$ such that:

$$R_{1}(x) = P(x) - \frac{p_{m}}{q_{n}} x^{m-n} Q(x) = [0, 1] \cdot \begin{bmatrix} 0 & 1 \\ 1 - \frac{p_{m}}{q_{n}} \end{bmatrix} \cdot \begin{bmatrix} P(x) \\ x^{m-n} Q(x) \end{bmatrix} \quad (0.5)$$

If we take into account the result in corollary 1, we will have:

$$R_1(x) = [0, 1] \cdot \begin{bmatrix} 0 & 1 \\ 1 & -\frac{p_m}{q_n} \end{bmatrix} \cdot D_m \cdot S_{\mathcal{D}} \cdot \underline{e}_m(x) = \underline{v}^t \cdot C \cdot D_m \cdot S_{\mathcal{D}} \cdot \underline{e}_m(x) \quad (0.6)$$

where $\underline{v}^t = [0, 1], C = \begin{bmatrix} 0 & 1 \\ 1 - \frac{p_m}{q_n} \end{bmatrix}$, D_m is the basis matrix of the polynomials P(x) and Q(x) and S_D the respective shifting matrix. Therefore, there exists a matrix $E_1 \in \mathbb{R}^{2 \times (m+1)}$ such that:

$$E_1 = C \cdot D_m \cdot S_{\mathcal{D}}$$
 and $R_1(x) = \underline{v}^t \cdot E_1 \cdot \underline{e}_m(x)$ (0.7)

We consider now the basis matrix D_m of the polynomials P(x) and Q(x):

$$D_m = \begin{bmatrix} P(x) \\ Q(x) \end{bmatrix} = \begin{bmatrix} p_m \dots p_{n+1} \ p_n \ p_{n-1} \dots p_0 \\ 0 \ \dots \ 0 \ q_n \ q_{n-1} \ \dots \ q_0 \end{bmatrix} \cdot \underline{e}_m(x)$$
(0.8)

and we will show that the above matrix E_1 is produced by applying the ERES operations to the basis matrix D_m of the polynomials P(x) and Q(x). We follow the next methodology:

1. We apply shifting on the rows of D_m . Let $S_{\mathcal{D}} \in \mathbb{R}^{(m+1)\times(m+1)}$, be the proper shifting matrix: $D_m^{(1)} = D_m \cdot S_{\mathcal{D}} = \begin{bmatrix} p_m \dots p_{m-n+1} p_{m-n} p_{m-n-1} \dots p_0 \\ q_n \dots q_1 & q_0 & 0 & \dots 0 \end{bmatrix}$ 2. We reorder the rows of the matrix $D_m^{(1)}$. If $J = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is the permutation matrix, then: $D_m^{(2)} = J \cdot D_m^{(1)} = \begin{bmatrix} q_n \dots q_1 & q_0 & 0 & \dots & 0 \\ p_m \dots p_{m-n+1} p_{m-n} p_{m-n-1} \dots p_0 \end{bmatrix}$

3. We apply stable row operations on
$$D_m^{(2)}$$
 (LU factorization). If $L = \begin{bmatrix} 1 & 0 \\ \frac{p_m}{q_n} & 1 \end{bmatrix}$
then $L^{-1} = \begin{bmatrix} 1 & 0 \\ -\frac{p_m}{q_n} & 1 \end{bmatrix}$ and therefore:

$$D_m^{(3)} = L^{-1} \cdot D_m^{(2)} = \begin{bmatrix} 1 & 0 \\ -\frac{p_m}{q_n} & 1 \end{bmatrix} \cdot \begin{bmatrix} q_n & \dots & q_1 & q_0 & 0 & \dots & 0 \\ p_m & \dots & p_{m-n+1} & p_{m-n-1} & \dots & p_0 \end{bmatrix}$$
$$= \begin{bmatrix} q_n & \dots & q_1 & q_0 & 0 & \dots & 0 \\ 0 & \dots & p_{m-n+1} - q_1 \frac{p_m}{q_n} & p_{m-n} - q_0 \frac{p_m}{q_n} & p_{m-n-1} & \dots & p_0 \end{bmatrix}$$

We notice that the term $\frac{p_m}{q_n}$ emerges from the LU factorization.

The above process can be described by the following equation:

$$D_m^{(3)} = L^{-1} \cdot J \cdot D_m \cdot S_\mathcal{D} \tag{0.9}$$

which represents the ERES methodology. Obviously $L^{-1} \cdot J = C$ and therefore, we conclude that $D_m^{(3)} \equiv E_1$.

The following theorem establishes the connection between the ERES method and the Euclidean Division of two real polynomials.

Theorem 2 (Matrix representation of the remainder of the Euclidean Division). Applying the algorithm of the Euclidean Division to a pair $\mathcal{D} = (P(x), Q(x)) \in \mathcal{D}_{m,n}$ of real polynomials, there are polynomials $G(x), R(x) \in \mathbb{R}[x]$ with degrees $deg\{G(x)\} = m - n$ and $0 \leq deg\{R(x)\} < n$ respectively, such that:

$$P(x) = G(x)Q(x) + R(x)$$

Then, the final remainder R(x) can be represented in matrix form as:

$$R(x) = \underline{v}^t \cdot E_N \cdot \underline{e}_m(x)$$

where $E_N \in \mathbb{R}^{2 \times (m+1)}$ is the matrix, which occurs from the successive application of the ERES operations on the basis matrix D_m of the pair \mathcal{D} and $\underline{v} = [0, 1]^t$.

The proof of the previous theorem is based on the iterative application of the result from proposition 1 to the sequence $\{(P(x), Q(x)), (R_i(x), Q(x))\}$, for $1 \leq i \leq (m-n)$. Therefore, we get a sequence of matrices $E_i = L_i^{-1} \cdot E_{i-1} \cdot S_i$, for $i = 1, 2, \ldots, N < m-n$, where the final matrix E_N gives the total remainder R(x) and every matrix L_i gives a specific coefficient of the quotient G(x).

References

- Christou, D., Karcanias, N., Mitrouli, M.: The matrix representation of the Euclidean Algorithm using the ERES methodology. Systems & Control Engineering Centre. Research Report (May 2008). City University, London, U.K.
- Gantmacher, F.R.: The Theory of Matrices. Volume I & II. Chelsea Publishing Company. New York, N.Y. (1959)
- 3. Karcanias, N.: Invariance properties and characterisation of the greatest common divisor of a set of polynomials. Int. Journ. Control **46** (1987) 1751–1760
- 4. Mitrouli, M., Karcanias, N.: Computation of the GCD of polynomials using Gaussian transformation and shifting. Int. Journ. Control **58** (1993) 211–228

71