Applied Mathematics E-Notes, 11(2011), 249–254 © ISSN 1607-2510
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/

Polynomial Division By Convolution*

Feng Cheng Chang†

Received 9 March 2011

Abstract

The division of a pair of given polynomials to find its quotient and remainder is derived by utilizing their convolution matrices. This process is simple, efficient and direct, when compared to the familiar classical longhand division and synthetic division.

1 Introduction

Before explaining our method, a polynomial multiplication method is to be briefly reviewed. Let

$$p(x) = b(x)a(x) = a(x)b(x),$$

where the polynomial $p(x)$ of degree $n+m$ is the product of a pair of given polynomials $a(x)$ and $b(x)$ of degrees m and n, respectively,

$$a(x) = \sum_{\ell=0}^{m} a_\ell x^{m-\ell},\ a_0 \neq 0,$$

$$b(x) = \sum_{\ell=0}^{n} b_\ell x^{n-\ell},\ b_0 \neq 0,$$

and

$$p(x) = \sum_{\ell=0}^{n+m} p_\ell x^{n+m-\ell}.$$

If we let $C(d)$ be the convolution matrix [1–3] associated with the column vector

*Mathematics Subject Classifications: 20F05, 20F10, 20F55, 68Q42.

†Allwave Corporation, Torrance, CA 90503, USA

$\mathbf{d} = (d_0, d_1, ..., d_t)^\dagger$, that is,

$$C(d) = \begin{bmatrix} d_0 & 0 & & \\ d_1 & \ddots & \ddots & \\ \vdots & \ddots & \ddots & 0 \\ \vdots & & \ddots & d_0 \\ \vdots & & & d_1 \\ d_t & & & \vdots \\ 0 & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ & & 0 & d_t \end{bmatrix},$$

then it is easily verified that the coefficient vectors

$$\mathbf{p} = (p_0, p_1, ..., p_{n+m})^\dagger, \mathbf{a} = (a_0, a_1, ..., a_m)^\dagger \text{ and } \mathbf{b} = (b_0, b_1, ..., b_n)^\dagger$$

of the polynomials $p(x)$, $a(x)$ and $b(x)$ respectively satisfy the relation

$$C(\mathbf{b}) \cdot \mathbf{a} = C(\mathbf{a}) \cdot \mathbf{b} = \mathbf{p},$$

and that

$$p_k = \sum_{\ell=\max(0,\, k-n)}^{\min(0,\, m)} b_{k-\ell} a_\ell = \sum_{\ell=\max(0,\, k-m)}^{\min(0,\, n)} a_{k-\ell} b_\ell,\ k = 0, 1, ..., n+m.$$

Using a similar technique, the division of a pair of polynomials will be developed. Let

$$\frac{b(x)}{a(x)} = q(x) + \frac{r(x)}{a(x)}$$

or

$$b(x) = a(x)\, q(x) + r(x)$$

where $b(x)$ and $a(x)$ are the given dividend and divisor of degrees n and m, $n \geq m$, and $q(x)$ and $r(x)$ are the resulting quotient and remainder respectively,

$$q(x) = \sum_{\ell=0}^{n-m} q_\ell x^{n-m-\ell},$$

and

$$r(x) = \sum_{\ell=0}^{m-1} r_\ell x^{m-1-\ell}.$$

Likewise with a little more manipulation, the polynomial division may be expressed in a matrix form with entries of $\mathbf{q} = (q_0, q_1, ..., q_{n-m})^\dagger$ and $\mathbf{r} = (r_0, r_1, ..., r_{m-1})^\dagger$ being respectively the coefficient vectors of the polynomials $q(x)$ and $r(x)$,

$$\begin{bmatrix} C(\mathbf{a}) & \begin{matrix} 0 \\ I \end{matrix} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{q} \\ \mathbf{r} \end{bmatrix} = \mathbf{b}.$$

The process involves a convolution matrix, so we shall name it "convolution polynomial division" or "polynomial division by convolution." This linear algebraic equation in matrix form may explicitly be written as

$$\begin{bmatrix} a_0 & & & & 0 & & & \\ \vdots & \ddots & & & & \ddots & & \\ \vdots & & \ddots & & & & \ddots & \\ \vdots & & & a_0 & & & & 0 \\ \vdots & & & \vdots & 1 & & & \\ a_m & & & \vdots & & \ddots & & \\ & \ddots & & \vdots & & & \ddots & \\ & & \ddots & \vdots & & & & \ddots \\ & & & a_m & & & & 1 \end{bmatrix} \begin{bmatrix} q_0 \\ \vdots \\ \vdots \\ q_{n-m} \\ r_0 \\ \vdots \\ \vdots \\ \vdots \\ r_{m-1} \end{bmatrix} = \begin{bmatrix} b_0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ b_n \end{bmatrix}.$$

Since $a_0 \neq 0$, the square matrix of the linear equation is non-singular; the desired solutions can thus be uniquely solved. We may also separate it into two parts for computing $\mathbf{q}$ and $\mathbf{r}$:

$$\frac{1}{a_0} \begin{bmatrix} a_0 & & & & & \\ b_0 & 0 & & & & \\ \vdots & -a_1 & \ddots & & & \\ \vdots & \vdots & \ddots & \ddots & & \\ \vdots & \vdots & & \ddots & \ddots & \\ b_{n-m} & -a_{n-m} & \cdots & \cdots & -a_1 & 0 \end{bmatrix} \begin{bmatrix} c \\ cq_0 \\ \vdots \\ \vdots \\ \vdots \\ cq_{n-m} \end{bmatrix} = \begin{bmatrix} c \\ cq_0 \\ \vdots \\ \vdots \\ \vdots \\ cq_{n-m} \end{bmatrix}$$

$$\begin{bmatrix} b_{n-m+1} & -a_{n-m+1} & \cdots & \cdots & \cdots & -a_1 \\ \vdots & \vdots & & & & \vdots \\ \vdots & -a_m & & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ b_n & & & & \ddots & -a_m \end{bmatrix} \begin{bmatrix} c \\ cq_0 \\ \vdots \\ \vdots \\ \vdots \\ cq_{n-m} \end{bmatrix} = \begin{bmatrix} cr_0 \\ \vdots \\ \vdots \\ \vdots \\ cr_{m-1} \end{bmatrix}$$

where c is a non-zero arbitrary constant, which may be set to $c = 1$. The vector $\mathbf{q}$ must be calculated consecutively in the element entry order, and the vector $\mathbf{r}$ may then be directly computed by simple matrix multiplication. When both **a** and **b** are integer vectors, we may set $c = a_0^{n-m+1}$ so that the computed matrix entries are all integers. Then the entire process becomes pure integer arithmetic operations, such that the round off errors may be completely eliminated.

The corresponding computer scheme may also be coded in the MATLAB environment. The inputs **b** and **a**, and the outputs **q** and **r** are the coefficient vectors of the given dividend $b(x)$ and divisor $a(x)$, and the resulting quotient $q(x)$ and remainder $r(x)$ respectively. The input c is an optional parameter and generally we set $c = 1$. However, if the given **b** and **a** are integer vectors, we may set $c = 0$. Then $c\mathbf{q}$ and $c\mathbf{r}$ are all in integer form, such that the computational round off errors may be eliminated.

Algorithm:

```
function [q,r,qc,rc] = polydiv_conv(b,a,c)
% Polynomial division by convolution.
n = length(b); m = length(a);
if m > n, q = 0; r = b; qc = 0; rc = b; c = 1; return; end;
if nargin < 3, c == 1; end;
w(1) = 1; if c == 0, w(1) = a(1)^(n-m+1); end;
for k = 2:n-m+2,
w(k) = [b(k-1),-a(min(k-1,m):-1:2)]*[w(1),w(max(2,k+1-m):k-1)]'/a(1);
end
for k = n-m+3:n+1,
w(k) = [b(k-1),-a(min(m,k-1):-1:k-1+m-n)]*[w(1),w(max(k+1-m,2):n-m+2)]';
end;
c = w(1);
qc = w(2:n-m+2);
rc = w(n-m+3:n+1);
q = qc/c;
r = rc(min(find(abs(rc)>0)):end)/c;
```

2 Illustrations with Remarks

For given

$$b(x) = 4x^8 + 5x^7 - x^6 + 7x^5 - 6x^4 + x^3 + 2x^2 - 3x + 7$$

and

$$a(x) = 3x^5 + x^4 - 7x^3 + 5x^2 - 4x + 2$$

in

$$\frac{b(x)}{a(x)} = q(x) + \frac{r(x)}{a(x)}$$

we shall find

$$q(x) = \frac{4}{3}x^3 + \frac{11}{9}x^2 + \frac{64}{27}x + \frac{176}{81}$$

and

$$r(x) = \frac{619}{81}x^4 + \frac{533}{81}x^3 - \frac{148}{81}x^2 + \frac{77}{81}x + \frac{215}{81}$$

by applying either one of the following approaches:

(i) Longhand polynomial division:

$$
\begin{array}{r|rrrrrrrrr}
 & +\frac{4}{3} & +\frac{11}{9} & +\frac{64}{27} & +\frac{176}{81} & & & & & \\
\hline
3+1-7+5-4+2 & +4 & +5 & -1 & +7 & -6 & +1 & +2 & -3 & +7 \\
 & +4 & +\frac{4}{3} & -\frac{28}{3} & +\frac{20}{3} & -\frac{16}{3} & +\frac{8}{3} & & & \\
\hline
 & & +\frac{11}{3} & +\frac{25}{3} & +\frac{1}{3} & -\frac{2}{3} & -\frac{5}{3} & +2 & -3 & +7 \\
 & & +\frac{11}{3} & +\frac{11}{9} & -\frac{77}{9} & +\frac{55}{9} & -\frac{44}{9} & +\frac{22}{9} & & \\
\hline
 & & & +\frac{64}{9} & +\frac{80}{9} & -\frac{61}{9} & +\frac{29}{9} & -\frac{4}{9} & -3 & +7 \\
 & & & +\frac{64}{9} & +\frac{64}{27} & -\frac{448}{27} & +\frac{320}{27} & -\frac{256}{27} & +\frac{128}{27} & \\
\hline
 & & & & +\frac{176}{27} & +\frac{265}{27} & -\frac{233}{27} & +\frac{244}{27} & -\frac{209}{27} & +7 \\
 & & & & +\frac{176}{27} & +\frac{176}{81} & -\frac{1232}{81} & +\frac{880}{81} & -\frac{704}{81} & +\frac{352}{81} \\
\hline
 & & & & & +\frac{619}{81} & +\frac{533}{81} & -\frac{148}{81} & +\frac{77}{81} & +\frac{215}{81}
\end{array}
$$

(ii) Synthetic polynomial division:

$$
\begin{array}{r|rrrr|rrrrr}
 & +4 & +5 & -1 & +7 & -6 & +1 & +2 & -3 & +7 \\
-\frac{1}{3} & & -\frac{4}{3} & -\frac{11}{9} & -\frac{64}{27} & -\frac{176}{81} & & & & \\
+\frac{7}{3} & & & +\frac{28}{3} & +\frac{77}{9} & +\frac{448}{27} & +\frac{1232}{81} & & & \\
-\frac{5}{3} & & & & -\frac{20}{3} & -\frac{55}{9} & -\frac{320}{27} & -\frac{880}{81} & & \\
+\frac{4}{3} & & & & & +\frac{16}{3} & +\frac{44}{9} & +\frac{256}{27} & +\frac{704}{81} & \\
-\frac{2}{3} & & & & & & -\frac{8}{3} & -\frac{22}{9} & -\frac{128}{27} & -\frac{352}{81} \\
\hline
 & +4 & +\frac{11}{3} & +\frac{64}{9} & +\frac{176}{27} & +\frac{619}{81} & +\frac{533}{81} & -\frac{148}{81} & +\frac{77}{81} & +\frac{215}{81}
\end{array}
$$

(iii) Convolution polynomial division:

$$
\frac{1}{3}\begin{bmatrix} 3 & & & & \\ +4 & 0 & & & \\ +5 & -1 & 0 & & \\ -1 & +7 & -1 & 0 & \\ +7 & -5 & +7 & -1 & 0 \end{bmatrix}
\begin{bmatrix} 1 \\ +4/3 \\ +11/9 \\ +64/27 \\ +176/81 \end{bmatrix}
=
\begin{bmatrix} 1 \\ +4/3 \\ +11/9 \\ +64/27 \\ +176/81 \end{bmatrix}
$$

$$
\begin{bmatrix} -6 & +4 & -5 & +7 & -1 \\ +1 & -2 & +4 & -5 & +7 \\ +2 & & -2 & +4 & -5 \\ -3 & & & -2 & +4 \\ +7 & & & & -2 \end{bmatrix}
\begin{bmatrix} 1 \\ +4/3 \\ +11/9 \\ +64/27 \\ +176/81 \end{bmatrix}
=
\begin{bmatrix} +619/81 \\ +533/81 \\ -148/81 \\ +77/81 \\ +215/81 \end{bmatrix}
$$

which may also be coverted schematically into the simpler form

$$
\begin{array}{r|rrrr|rrrrr}
1 & +4 & +5 & -1 & +7 & -6 & +1 & +2 & -3 & +7 \\
 & 0 & -1 & +7 & -5 & +4 & -2 & & & \\
 & & 0 & -1 & +7 & -5 & +4 & -2 & & \\
 & & & 0 & -1 & +7 & -5 & +4 & -2 & \\
 & & & & 0 & -1 & +7 & -5 & +4 & -2 \\
\hline
1 & +\frac{4}{3} & +\frac{11}{9} & +\frac{64}{27} & +\frac{176}{81} & +\frac{619}{81} & +\frac{533}{81} & -\frac{148}{81} & +\frac{77}{81} & +\frac{215}{81}
\end{array}
$$

or

3^4	+4	+5	−1	+7	−6	+1	+2	−3	+7
	0	−1	+7	−5	+4	−2			
		0	−1	+7	−5	+4	−2		
			0	−1	+7	−5	+4	−2	
				0	−1	+7	−5	+4	−2
81	+108	+99	+192	+176	+619	+533	−148	+77	+215

In view of the three approaches in this example, the convolution polynomial division seems to be simple and effective. The desired quotient and reminder are readily determined without computing any intermediate values as in the familiar classical longhand polynomial division and synthetic polynomial division.

References

[1] B. Dayton, Polynomial GCDs by Linear Algebra, Theory of Equations, Northeastern Illinois University, 2004.

[2] Z. Zeng, Computing multiple roots of inexact polynomials, Math. Comput., 74(2005), 869–903.

[3] F. C. Chang, Solving multiple-roots polynomials, IEEE Antennas and Propagation Magazine, 51(2009), 151–155.