

A proof of the correctness of synthetic division

We consider the problem of dividing the polynomial $a(x) = \sum_{k=0}^n a_k x^k$ ($a_n \neq 0$) by the polynomial $b(x) = \sum_{k=0}^m b_k x^k$ ($b_m \neq 0$), where $0 \leq m \leq n$. Synthetic division arranges the coefficients of a and b in a table as follows:

| | | | | | | | | |
|--|------------|------------|----------|--------|--------|-----------|----------|-------|
| | | | | | a_n | a_{n-1} | \cdots | a_0 |
| | | | | $-b_0$ | | | | |
| | | | \ddots | | | | | |
| | | $-b_{m-2}$ | | | | | | |
| | $-b_{m-1}$ | | | | | | | |
| | | | | | | | | |
| | | | | | $/b_m$ | | | |

Division then proceeds as illustrated below (the left side of the table has been condensed for the sake of space),

| | | | | | | | | | |
|------------|-----------|--------------------|----------------------|----------|----------------|----------------|----------------|----------|------------|
| $-b_0$ | a_n | a_{n-1} | a_{n-2} | \cdots | a_m | a_{m-1} | a_{m-2} | \cdots | a_0 |
| \vdots | | | | \cdots | \cdots | \cdots | \cdots | \cdots | $-b_0 c_0$ |
| $-b_{m-2}$ | | | $-b_{m-2} c_{n-m}$ | \cdots | $-b_{m-2} c_2$ | $-b_{m-2} c_1$ | $-b_{m-2} c_0$ | | |
| $-b_{m-1}$ | | $-b_{m-1} c_{n-m}$ | $-b_{m-1} c_{n-m-1}$ | \cdots | $-b_{m-1} c_1$ | $-b_{m-1} c_0$ | | | |
| | a_n | $\sum \cdots$ | $\sum \cdots$ | \cdots | $\sum \cdots$ | d_{m-1} | d_{m-2} | \cdots | d_0 |
| $/b_m$ | c_{n-m} | c_{n-m-1} | c_{n-m-2} | \cdots | c_0 | | | | |

where the entry immediately below the bar in each column is the sum of the entries above the bar in that column, and the entry in the last row is this sum divided by b_m . The quotient is then $c(x) = \sum_{k=0}^{n-m} c_k x^k$, and the remainder is $d(x) = \sum_{k=0}^{m-1} d_k x^k$.

Note: In the following proof, we will regard b_k as zero if $k < 0$ or $k > m$; similarly, we will regard c_k as zero if $k < 0$ or $k > n - m$. Sums are to be understood as ranging over all integers unless otherwise specified.

From the illustration, it is clear that

$$d_k = a_k + \sum_{i+j=k} -b_i c_j = a_k - \sum_i b_i c_{k-i}, \quad 0 \leq k < m;$$

$$b_m c_k = a_{k+m} + \sum_{\substack{i+j=k+m; \\ i \leq m-1}} -b_i c_j = a_{k+m} - \sum_{i \leq m-1} b_i c_{k+m-i}, \quad 0 \leq k \leq n - m.$$

To prove the correctness of synthetic division, we must show that $b(x)c(x) + d(x) = a(x)$. We do so by comparing the coefficients of both polynomials. The coefficient of x^k in $b(x)c(x) + d(x)$

is clearly

$$\left(\sum_i b_i c_{k-i} \right) + d_k,$$

which, for $0 \leq k < m$, is equal to

$$\left(\sum_i b_i c_{k-i} \right) + \left(a_k - \sum_i b_i c_{k-i} \right) = a_k.$$

On the other hand, if $m \leq k \leq n$, the coefficient of x^k in $b(x)c(x) + d(x)$ is

$$\begin{aligned} b_m c_{k-m} + \sum_{i \neq m} b_i c_{k-i} &= \left(a_k - \sum_{i \leq m-1} b_i c_{k-i} \right) + \sum_{i \neq m} b_i c_{k-i} \\ &= a_k + \sum_{i \geq m+1} b_i c_{k-i} \\ &= a_k, \end{aligned}$$

which completes the proof.