Travaux Dirigés Polynomials n°2

Combinatorics and Computer Algebra Lecture

—MPRI master's—

Fast Division / Newton's Method / Applications

Euclidean division between higher-degree polynomials is a very slow operation. The aim of this tutorial is to look at a faster method based on multiplication.

1 Fast division

▸ Exercice 1. Standard Euclidean division

Let A and B be two polynomials ($B \neq 0$). Remember that there is a *unique* pair of polynomials Q and R called the quotient and the remainder for which

$$A = B\,Q + R \qquad \text{and} \qquad \deg(R) < \deg(B)\,. \tag{1}$$

1. In the worst case, based on $\deg(A)$ and $\deg(B)$, how many coefficient multiplications need to take place during the Euclidean division of A by B ?

▸ Exercice 2. Newton's method

Newton's method is an iterative algorithm for solving the equation $f(x) = 0$, as the limit of a sequence defined by (see Newton's Method on Wikipedia) :

$$x_{k+1} = x_k + \frac{f(x_k)}{f'(x_k)} \tag{2}$$

Here the equation takes the form $f(x) = \frac{1}{x} - a$ where a is a constant and x is the unknown. We thus find

$$f'(x) = -\frac{1}{x^2} \qquad \textit{and} \qquad x_{n+1} = x_n - \frac{\frac{1}{x_n} - a}{-\frac{1}{x_n^2}} = 2x_n - a x_n^2 \tag{3}$$

If we are working with complex numbers rather than polynomials, this sequence converges if $|a-1| < 1$. We can thus easily see that the limit is $\frac{1}{a}$.

Let us apply this idea to polynomials. We assume that F is a polynomial such that $F(0) = 1$. We define by induction the sequence $(G_i)_{i\geq 0}$ of polynomials by

$$G_0(0) = 1 \qquad \text{and} \qquad G_{i+1} = 2G_i - F G_i^2 \quad \text{for } i \geq 0\,. \tag{4}$$

2. Calculate the first values of the sequence G_i for $F = X + 1$ and $F = 1 + aX$ where a is a fixed constant.
3. Show that there is a polynomial H_i for any i such that

$$F G_i = 1 + X^{2^i} H_i\,. \tag{5}$$

4. Deduce from this that $G_{i+1} - G_i$ is a polynomial multiple of X^{2^i}. In particular, we don't need to calculate coefficients of degree below 2^i when calculating G_{i+1}.

▸ **Exercice 3. Fast division algorithm** Let $A = \sum_{i=0}^{m} a_i X^i$, a polynomial of degree m. For $k \geq m$, we define the polynomial $\mathrm{Rev}_k(A)$ as

$$\mathrm{Rev}_k(A) := X^k A\left(\frac{1}{X}\right). \tag{6}$$

5. What are the coefficients of $\mathrm{Rev}_m(A)$?
6. Let B, a polynomial of degree $n \leq m$. Let Q and R be the quotient and the remainder of the Euclidean division of A by B. Show that
$$\mathrm{Rev}_m(A) = \mathrm{Rev}_n(B)\,\mathrm{Rev}_{m-n}(Q) + X^{m-n+1}\,\mathrm{Rev}_{n-1}(R). \tag{7}$$
7. For $A = X^3 + 2X + 3$ and $B = X^2 + X$, give an example of the equation above.
8. Using the previous exercise, show that we can find polynomials S and T such that
$$1 = \mathrm{Rev}_n(B)S + X^{m-n+1}T. \tag{8}$$
9. Deduce from this an algorithm for calculating Q and then R without Euclidean division.
10. Apply the method to the polynomials A and B.
11. How many coefficient multiplications are required by this method ?

2 Application to multi-point evaluation

Let $P(X) := \sum_{i=0}^{d} c_i X^i$, a polynomial of degree d. We assume n points $a_1, \ldots, a_n$. We want to calculate the values $P(a_i)$ for $i = 1 \ldots n$ as quickly as possible.

1. If we calculate the polynomial values independently at each point using Horner's method, how many coefficient multiplications do we need to do ?

We will look at a faster method based on Euclidean division.

2. First calculate the remainder and quotient of the division of $P := X^4 + 2X^2 - 3X + 1$ by $X - 3$ and then calculate $P(3)$. What do you notice ?
3. More generally, show that the remainder dividing the polynomial $P(X)$ by a polynomial $X - a$ is a constant polynomial equal to $P(a)$.
4. Show that if $B = B_1 B_2$ is the product of two polynomials, then the remainder R_1 of the division of P by B_1 is equal to the remainder of the division of R by B_1 where R is the remainder of the division of P by B. In other words, if we note the remainder of the division of U by V as $U \mod V$, we have
$$\text{if } B_1 \text{ divides } B, \text{ then} \qquad P \mod B_1 = (P \mod B) \mod B_1.$$

Evaluation

So to calculate the values of P for 3 and 5 we can proceed as follows :

— Let $B_1 = X - 1$ and $B_2 = X - 3$. We expand the polynomial $B := B_1 B_2 = (X - 1)(X - 3)$.

— We calculate $R = P \mod B$.

— We calculate $R_1 = R \mod B_1$ and $R_2 = R \mod B_2$.

5. Perform the calculations in the example and check the results.
6. Compare the number of coefficient multiplications for the three methods (Horner, two divisions, iterated division).

This algorithm can be generalised to cases of n points using a divide and conquer method.

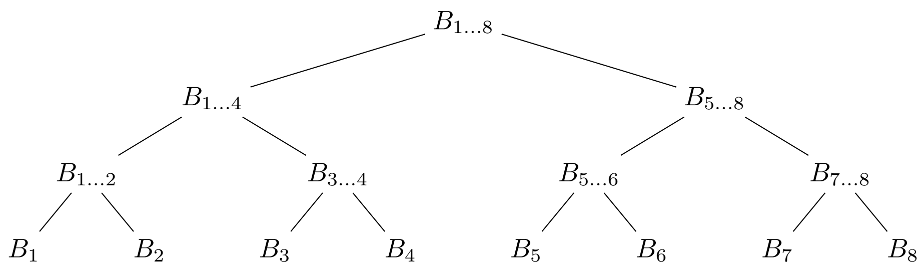
7. Find a method for four points.

General algorithm

We now consider the case of any number of points. Initially, to simplify, we can assume that the number n of points is a power of 2. This allows us to use a binary tree structure. We will use the following notation :

$$B_{i\ldots j} := (X - a_i)(X - a_{i+1}) \ldots (X - a_j) \,. \tag{9}$$

In the case of a single point we have $B_{i\ldots i} = B_i = (X - a_i)$. We then organise the calculation according to a tree of the following form (in this case $n = 8$) :



8. Describe the algorithm for calculating the various B values. Note that if we want to calculate the values for the a_i of different polynomials P, we only need to do this first calculation once.
9. Describe the algorithm for evaluating $P(a_i)$ by successive Euclidean division.
10. Apply the algorithm to calculate the values of P for $1, 3, 4, 5$.
11. Compare the worst-case number of coefficient multiplications for the three methods (Horner, n divisions, iterated division) if the number of points is $n = 2, 4, 8, 16, 32$.