EXERCISE FOR CSE202 – WEEK 2

The starting point in the presentation of Karatsuba's algorithm in the course is that a polynomial of degree 2 can be reconstructed from its values at 3 points. The aim of this exercise is to analyze how generalizations of this idea lead to faster multiplication algorithms.

Observe first more generally that given $k+1$ points $(a_0, \dots, a_k)$ and a polynomial $P = p_0 + \dots + p_k x^k$, the values of P at these points are given by the product

$$\begin{pmatrix} P(a_0) \\ \vdots \\ P(a_k) \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & a_0 & \cdots & a_0^k \\ & \cdots & \cdots & \\ 1 & a_k & \cdots & a_k^k \end{pmatrix}}_{V(a_0,\dots,a_k)} \begin{pmatrix} p_0 \\ \vdots \\ p_k \end{pmatrix}.$$

The matrix $V(a_0, \dots, a_k)$ is known as a Vandermonde matrix and it is invertible when the a_i's are all distinct. In that case, multiplication by the inverse V^{-1} solves the interpolation problem: it recovers the coefficients of a polynomial from its values at $(a_0, \dots, a_k)$.

We first clarify the use of this idea by designing a variant of Karatsuba's algorithm. With the three points $\{-1, 0, 1\}$, the inverse of the Vandermonde matrix is

$$V(-1,0,1)^{-1} = \frac{1}{2}\begin{pmatrix} 0 & 2 & 0 \\ -1 & 0 & 1 \\ 1 & -2 & 1 \end{pmatrix}.$$

This implies that for any polynomial P of degree at most 2,

$$P(T) = \frac{1}{2}\left(2P(0) + (P(1) - P(-1))T + (P(1) - 2P(0) + P(-1))T^2\right).$$

Question 1. *By proceeding as in the derivation of Karatsuba's algorithm in the lecture, design a recursive algorithm for polynomial multiplication that relies on this formula. Give its asymptotic complexity.*

Hint. *Split the two input polynomials F and G exactly as in Karatsuba, $F = F_0 + x^k F_1$ and $G = G_0 + x^k G_1$, and apply the interpolation approach presented above.*

Next, we consider the five points $-2, -1, 0, 1, 2$. While the details are unimportant, it may fix the ideas to see the inverse

$$V(-2,-1,0,1,2)^{-1} = \frac{1}{24}\begin{pmatrix} 0 & 0 & 24 & 0 & 0 \\ 2 & -16 & 0 & 16 & -2 \\ -1 & 16 & -30 & 16 & -1 \\ -2 & 4 & 0 & -4 & 2 \\ 1 & -4 & 6 & -4 & 1 \end{pmatrix}.$$

Question 2. *Proceeding as before, but now splitting the polynomials to be multiplied into three rather than two parts, give the outline of a recursive algorithm for polynomial multiplication. It is not necessary to write explicitly the coefficients used at each step, but the information should be sufficient for you to show that its* *complexity obeys the recurrence $C(n) \leq 5C(\lceil n/3 \rceil) + \lambda n$, from which you should deduce the asymptotic complexity of your algorithm and see that it improves upon Karatsuba's algorithm.*

Hint. *Split the two input polynomials F and G as $F = F_0 + x^k F_1 + x^{2k} F_2$ and $G = G_0 + x^k G_1 + x^{2k} G_2$, and apply the interpolation approach presented above, which now concerns a product of degree 2 polynomials.*

Question 3. *Without entering into any detail, give the outline of a generalization of this method that would split each polynomial into m parts recursively, for a given m. Its special cases when $m = 2, 3$ should correspond to the algorithms of the previous questions. Indicate its complexity in the form $O(n^{f(m)})$ for some f to be determined and give the limit of $f(m)$ as $m \to \infty$. Conclude on the complexity of multiplication.*