# TD 2: Polynomial multiplication

## Exercice 1. Polynomial Arithmetic

A polynomial $P = p_0 + p_1 X + \cdots + p_{n-1} X^{n-1}$ by an array of $n$ elements $[p_0, p_1, \ldots, p_{n-1}]$.

**a.** Propose a *Divide and Conquer* algorithm for the multiplication of two polynomials of same degree.

Indication: one can use the identity:

$$(P_0 + XP_1)(Q_0 + XQ_1) = P_0Q_0 + X(P_0Q_1 + P_1Q_0) + X^2 P_1Q_1$$

**b.** Analyse its cost (when the size of the polynomials is a power of two).

**c.** In 1960, Karatsuba proposed to use instead the following formula:

$$(P_0 + XP_1)(Q_0 + XQ_1) = P_0Q_0 + X((P_0 + P_1)(Q_0 + Q_1) - P_0Q_0 - P_1Q_1) + X^2 P_1Q_1$$

Deduce an algorithm and analyse it complexity.

We now investigate the decomposition of polynomials in three: $P = P_0 + XP_1 + X^2P_2$ et $Q = Q_0 + XQ_1 + X^2Q_2$. Toom proposed a formula computing $P \times Q$ using the five following values:

$$\begin{array}{rcl} M_0 &=& P_0Q_0 \\ M_1 &=& (P_0 + P_1 + P_2)(Q_0 + Q_1 + Q_2) \\ M_2 &=& (P_0 - P_1 + P_2)(Q_0 - Q_1 + Q_2) \\ M_3 &=& (P_0 + 2P_1 + 4P_2)(Q_0 + 2Q_1 + 4Q_2) \\ M_4 &=& P_2Q_2 \end{array}$$

The product $R = P \times Q = R_0 + R_1X + R_2X^2 + R_3X^3 + R_4X^4$ is obtained as follows:

$$\left\{ \begin{array}{rcl} R_0 &=& M_0 \\ R_1 &=& \frac{1}{6}(-3M_0 + 6M_1 - 2M_2 - M_3 + 12M_4) \\ R_2 &=& \frac{1}{2}(-2M_0 + M_1 + M_2 - 2M_4) \\ R_3 &=& \frac{1}{6}(3M_0 - 3M_1 - M_2 + M_3 - 12M_4) \\ R_4 &=& M_4 \end{array} \right. \tag{1}$$

**d.** What is the cost of the corresponding algorithm multiplying polynomials of arbitrary degrees?

**e.** Justify that the formulas computing the $M_i$ can be viewed as evaluations. State in which points?

**f.** Deduce how the coefficients of the formule (1) have been found.

More generally, Toom-Cook algorithms at order $k$ compute the product $P \times Q$ of two polynomials of size $k$ in $(2k - 1)$ multiplications.

**g.** What is the cost of these algorithms ?

**h.** Explain how to construct them.

**i.** Conclude on the cost of multiplying polynomials.