COMP3121: Assignment 2 – Q2

Gerald Huang

$z5209342$

Updated: June 17, 2020

Let $P(x) = A_0 + A_1 x^{100} + A_2 x^{200}$. Our goal is to show that $P(x)^2$ can be calculated with only five large integer multiplications. We observe that $P(x)$ can be written as $P(x) = A_0 + A_1 \left(x^{100}\right) + A_2 \left(x^{100}\right)^2$. So by setting $y = x^{100}$, we can write $P(x)$ using our substitution of y, namely $P(y) = A_0 + A_1 y + A_2 y^2$ and so we have converted $P(x)$ into an order 2 polynomial.

Define $Q(y) = P(y)^2 = B_0 + B_1 y + B_2 y^2 + B_3 y^3 + B_4 y^4$. We observe that $Q(y)$ will be a polynomial of degree 4 and so there requires 5 coefficients to uniquely define $Q(y)$. We will apply the value representation correspondence between coefficients and values of $Q(y)$ by the following relationship

$$Q(y) \leftrightarrow \{(y_0, Q(y_0)), (y_1, Q(y_1)), (y_2, Q(y_2)), (y_3, Q(y_3)), (y_4, Q(y_4))\},$$

where y_a ranges from -2 to 2.

But we realise that $Q(y_a)$ can be directly computed by $P(y_a)P(y_a)$ which can be arbitrarily large depending on our choice of y_a. Hence these five arbitrarily large multiplications of integers are enough to find partials of $Q(y)$. To extract the coefficients, apply the inverse Vandermonde matrix left multiplied with the coordinate vector of $Q(y)$ with elements $Q(y_0), Q(y_1), Q(y_2), \ldots, Q(y_4)$. That is, define

$$\begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \end{pmatrix} = \begin{pmatrix} 1 & -2 & (-2)^2 & (-2)^3 & (-2)^4 \\ 1 & -1 & (-1)^2 & (-1)^3 & (-1)^4 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2^2 & 2^3 & 2^4 \end{pmatrix}^{-1} \begin{pmatrix} Q(y_0) \\ Q(y_1) \\ Q(y_2) \\ Q(y_3) \\ Q(y_4) \end{pmatrix}.$$

Each of these calculations take constant time to calculate and are relatively small multiplications to calculate. Thus, it takes linear time to calculate the coordinates of $Q(y)$. This completes our construction of $Q(y)$ which is equivalently $P(y)^2$. So to extract the square of $P(x)$, we set $y = x^{100}$ which can be calculated by computing $Q(x^{100})$.