Reunion report 1

Simon Sepiol-Duchemin Joshua Setia

January 30, 2025

1 Recap of reunion

Studying roots of a polynomial on different intervals

For a polynomial (written as an array) $f = (f_0, ..., f_d) \in \mathbb{Z}^{d+1}$, we can bound its maximum real positive root with a function $Bound(\underline{f}) = B = 2^k$ (with B a power of 2).
By performing operations on x, we can reduce the interval bounding the roots $[0, B]$ to a new interval.

For example, by substituting x by $\frac{x}{2^k}$, we'll then study the real positive roots on the interval $[0, 1]$. The corresponding polynomial will be $f(\frac{x}{2^k}) \in \mathbb{Q}[x]$. We will then need to factorize f to have $\tilde{f} \in \mathbb{Z}[x]$, in order to have integers coefficients.

Recursive method

Using the method described above to study the roots on different intervals, we want to do it on specific intervals repeatedly until we've successfully isolated each root :

- $]0, 1[$ by doing the substitution $x \to \frac{x}{2^k}$
- $]0, +\infty[$ by doing the substitution $x \to \frac{1}{y+1}$
- $]0, \frac{1}{2}[$ by doing the substitution $x \to 2x$
- $]\frac{1}{2}, 1[$ by doing the substitution $x \to 2x$

Role of the Taylor Shifts

When doing the substitution $x \to \frac{1}{y+1}$, we will only need to perform a Taylor Shift, since doing $f(\frac{1}{x})$ does not require any operations. Indeed, for a polynomial $f = (f_0, ..., f_d)$:

$$f(\frac{1}{x}) = \frac{f_0 x^d + f_1 x^{d-1} + ... + f_d}{x^d}$$

Trivial cases

For specific values of x, verifiyng the number of real positive roots does not require any operations :

- $x = 0$, we only need to know if the least significant coefficient is zero
- $x = 1$, we only need to summ the coefficients

2 Tasks for next reunion

Implementations

Test flint's polynomial multiplication performance.
The tested polynomials must have integers coefficients, be univariate and dense (nonzero coefficients). Measure the performance by changing :

- the degree, with fixed coefficients size
- the coefficients size (up to thousands of bit), with fixed degree

Deduce which algorithms are used for the flint polynomial multiplication operation (naive, Karatsuba, Cantor and Kaltofen...).

Search and suggest

- Function $Bound(\underline{f})$ for bounding a polynomial's real positive roots
- Fast way of computing $f(\frac{1}{2})$, similar to $f(1)$ and $f(0)$, only using shifts

Understand, learn and be able to redo on board

- Decartes' rule of sign's proof
- Divide and conquer algorithm for Taylor Shifts