max planck institut informatik

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Michael Sagraloff **Winter term 2017/18**

Computer Algebra

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter17/comp-alg/

Assignment sheet 1 due: Monday, October 30

Exercise 1: Polynomial Evaluation (4 points)

Let $f = a_0 + \cdots + a_d \cdot x^d \in \mathbb{Z}[x]$ be a polynomial of degree d with integer coefficients of length at most L, and let $m \in \mathbb{Z}$ be an ℓ-digit number. Show that

(a) $f(m)$ is an $O(d\ell + L)$-digit number.

(b) computing $f(m)$ using the *Horner's method*

$$f(m) = a_0 + m \cdot (a_1 + m \cdot (a_2 + \cdots m \cdot (a_{d-1} + m \cdot a_d))$$

and the school method for multiplication takes $O(d \cdot \ell \cdot (d\ell + L)))$ primitive operations.

Exercise 2: Karatsuba / Toom-Cook multiplication (4 points)

For multiplying two n-digit integers a and b (wrt. to some base B), Karatsuba's method uses the fact that

$$\begin{aligned} a \cdot b = \quad & a^{(0)} \cdot b^{(0)} \\ & + \big((a^{(0)} + a^{(1)}) \cdot (b^{(0)} + b^{(1)}) - a^{(0)} \cdot b^{(0)} - a^{(1)} \cdot b^{(1)}\big) \cdot B^{\lceil n/2 \rceil} \\ & + a^{(1)} \cdot b^{(1)} \cdot B^{2\lceil n/2 \rceil}, \end{aligned} \tag{1}$$

where $a = a^{(0)} + a^{(1)} \cdot B^{\lceil n/2 \rceil}$ and $b = b^{(0)} + b^{(1)} \cdot B^{\lceil n/2 \rceil}$ with non-negative integers $a^{(i)}$ and $b^{(i)}$ of length at most $\lceil n/2 \rceil$.

(a) In each recursion step of Toom-Cook-k multiplication, a similar relation as in (1) is used. Choose any interpolation points $x_0, \ldots, x_4$ and provide a corresponding relation for Toom-Cook-3.

(b) How do we have to choose the interpolation points x_0, x_1, x_2 in Toom-Cook-2 to obtain exactly the same relation as in (1)?

(Hint: You may also choose interpolation points $x_i = \infty$ for some i, where we define $f(\infty) = a_d$ for an arbitrary polynomial $f(x) = a_0 + a_1 x + \cdots + a_d x^d$.)

Exercise 3: Gaussian elimination (4 points + 4 bonus points for $\star$)

Let $A = (a_{ij})_{1 \le i,j \le n}$ be an $n \times n$-matrix with integer entries a_{ij} of length L.

(a) Give an upper bound B for the length of the $\det A$ that is polynomial in n and L.

(b) We now consider Gaussian elimination with pivoting in order to compute $\det A$.

Let $A^{(0)} := A$ and $A^{(k)}$ be the matrix obtained after k elimination steps. $A^{(k)}$ has rational entries $a_{ij}^{(k)}$, and it holds that $a_{ii}^{(k)} \neq 0$ for all $i = 1, \dots, k$ and $a_{ij}^{(k)} = 0$ for all $i > j$ and $j = 1, \dots, k$.

The pivoting rule is as follows: Let r be the smallest row index with $r \geq k+1$ such that $a_{r,k+1}^{(k)} \neq 0$. If no such r exists, then $\det A = 0$ and we finish immediately. Otherwise, we exchange the row r with row $k+1$. This yields the matrix $\bar{A}^{(k)} = (\bar{a}_{ij}^{(k)})$. We then define

$$a_{ij}^{(k+1)} := \begin{cases} \bar{a}_{ij}^{(k)} & \text{for } i \leq k \text{ and} \\ \bar{a}_{ij}^{(k)} - \frac{\bar{a}_{i,k+1}^{(k)}}{\bar{a}_{k+1,k+1}^{(k)}} \cdot \bar{a}_{k+1,j}^{(k)} & \text{for } i \geq k+1. \end{cases}$$

- ⋆ Prove that, for any k and any $a_{ij}^{(k)}$ with $k+1 \leq i, j \leq n$, it holds that $a_{11}^{(k)} a_{22}^{(k)} \cdots a_{kk}^{(k)}$ as well as $a_{11}^{(k)} a_{22}^{(k)} \cdots a_{kk}^{(k)} \cdot a_{ij}^{(k)}$ can be written as the determinant of a submatrix of A, up to some unit factor (± 1).
- Conclude that all intermediate values created by the Gaussian elimination algorithm can be represented with a number of digits that is polynomial in L and n.
- Show A^{-1} has entries that can be represented with a number of digits that is polynomial in L and n.

Exercise 4: Box functions and root finding (4 points)

Let $f(x) = a_0 + a_1 x + \cdots + a_d x^d \in \mathbb{Z}[x]$ be an arbitrary polynomial with integer coefficients. Our goal is to count all real roots of f, provided that f has only simple roots.

(a) Show that all real roots of f have absolute value bounded by $M := 1 + \max_{0 \leq i < d} |\frac{a_i}{a_n}|$.

(b) Use box functions for f and its derivative f' to derive a method that allows you to decide whether a certain interval I contains no root or exactly one root. Your method may fail (with the output "I don't know"); however, it should succeed for sufficiently small intervals I.

(c) Formulate an algorithm to determine the number of real roots of f.

(Hint: By Rolle's theorem, any interval I which contains more than one root of f also contains a root of its derivative f'.)