Homework 1

Assigned: 3rd Feb; Due Date: 24th Feb

Discussion is encouraged, but please acknowledge it and write your answers independently.

Q.1 Given an n-bit number x, show that we can compute the number $\lfloor 2^{2n-1}/x \rfloor$ in $O(M(n))$ bit-operations, where $M(n)$ is the complexity of multiplying two n-bit numbers.

Q.2 Let $n_1, \ldots, n_k$ be positive integers. Show that

$$\sum_{i=1}^{k} \mathrm{len}(n_i) - k \leq \mathrm{len}\left(\prod_{i=1}^{k} n_i\right) \leq \sum_{i=1}^{k} \mathrm{len}(n_i).$$

Q.3 Given integers $n_1, \ldots, n_k$ with each $n_i > 1$, show that we can compute the product $N := \prod_{i=1}^{k} n_i$ in time $O(\mathrm{len}(N)^2)$.

Q.4 Given two integer polynomials $A(x), B(x)$, with coefficients of bit-length L. What is the bit-complexity of the following operations:

(a) Computing the product $A \times B$ using classical multiplication.

(b) Evaluating $A(x)$ at an integer of bit-size L' using Horner's method.

Q.5 Let R be a ring.

(a) Let $n = 2^k$. Show that for all $a \in R$

$$\sum_{i=0}^{n-i} a^i = \prod_{i=0}^{k-1} (1 + a^{2^i}).$$

(b) Let $n = 2^k$. For some $\omega \in R_{\neq 0}$, define $M := \omega^{n/2} + 1$. Using the result above show that for $1 \leq s < n$

$$\sum_{i=0}^{n-1} \omega^{is} \equiv 0 \mod M.$$

Q.6 Use the following observation to improve the running time of the simplified Schönhage-Strassen Algorithm: Let n_1, n_2 be relatively prime numbers and suppose $n \leq n_1 n_2$ is such that

$$n \equiv y_1 \mod n_1 \text{ and } n \equiv y_2 \mod n_2$$

then

$$n = y_1 n_2 (n_2^{-1} \mod n_1) + y_2 n_1 (n_1^{-1} \mod n_2).$$

Q.7 A D-Rep of a polynomial $A(x)$ is by its value and the values of all its derivatives at a point, i.e., given a point x_0 the representation is the sequence

$$(A(x_0), A'(x_0), \ldots, A^{(i)}(x_0), \ldots, A^{(n)}(x_0)),$$

where $n = \deg(A)$.

(a) Given a D-Rep of two polynomials, show how to add and multiply them.

(b) Give an algorithm to evaluate a polynomial given in D-Rep.

(c) Give an algorithm to convert between D-Rep and C-Rep (coefficient representation).

Q.8 Given a rational number $f \in [0,1]$, the **fGCD-problem** is as follows: given two polynomials A, B, compute a matrix $M := \mathtt{fGCD}(A,B)$ such that M applied to (A,B) gives us (A', B') such that

$$\deg(A') \geq f \deg(A) > \deg(B'),$$

that is, $\deg(A')$ and $\deg(B')$ straddle $f \deg(A)$. Show that $\mathtt{fGCD}(A,B)$ can be computed in the same complexity as $\mathtt{hGCD}(A,B)$ using it as a subroutine.

Q.9 Recall the definition of generalized PRS $A_0, A_1, \ldots, A_k$ based upon the sequence $\{\alpha_i\}$ and $\{\beta_i\}$ from the lectures. For $1 < j < k$, define the constants

$$\gamma := \left(\prod_{i=1}^{j-1} \beta_i^{n_{i+1}-n_j+1} \mathtt{lead}(A_{i+1})^{n_i - n_{i+2}}\right)$$

and

$$\eta := \left(\prod_{i=1}^{j-1} \alpha_i^{n_{i+1}-n_j+1}\right).$$

Show the following for $1 < j < k$

$$\begin{aligned} \eta S_{n_j - 1} &= \pm\gamma \ \mathtt{lead}(A_j)^{-\delta_{j+1}+1} \ A_{j+1}. \\ \eta S_{n_{j+1}} &= \pm\gamma \ \alpha_{j+1}^{\delta_{j+1}-1} \ A_{j+1}. \end{aligned} \tag{1}$$

Q.10 Consider the following specialization of generalized PRS: $\alpha_i := \mathtt{lead}(A_i)^{\delta_i + 1}$, the standard choice of α_i, $\beta_{i+1} := \alpha_i$, and $\beta_1 := 1$. Show that the polynomials in the PRS obtained are in $\mathbb{Z}[x]$.