CMPT 706 — Algorithms for Big Data

Homework Assignment 1

Instructor: Igor Shinkar *Due date: January 30, 2020 until midnight*

Submit your solutions, printed or written in readable handwriting, to the assignment boxes in CSIL.

Question 1 (20 points) *Let* $f\colon \mathbb{N} \to \mathbb{N}$ *be a function on positive integers that outputs positive integers. Suppose that* $f = O(n^3)$*, and* $f = \Omega(n^3)$*. Prove formally that* $f = \Theta(n^3)$*.*

Question 2 (20 points) *Consider the following algorithm.*

```
Input: Array $A$ of length $n$
for $i = 1 \ldots n$ do
    $j \leftarrow i$
    while $j < n$ do
        $j \leftarrow j * 2$
        Print $A[j]$
endwhile
```

Use big-O notation to express the runtime of‘the algorithm as a function of n*.*

Question 3 (20 points) *Suppose we have an algorithm that given two* n*-bit numbers* a, b *computes the product* $a \cdot b$ *in time* $O(n^{1.1})$ *Design an algorithm that gets a number* a *of length* n *and a number* b *of length* kn *for some parameter* k*, and computes the product* $a \cdot b$ *in time* $O(kn^{1.1})$*.*

Explain why the algorithm is correct, and prove the guarantee on the runtime.

Question 4 (20 points) *Show the execution of the Euclidean Algorithm for computing* $gcd(108, 135)$*. Write explicitly all intermediate steps of the algorithm.*

Question 5 (20 points) *In an RSA cryptosystem we have* $p = 67$*,* $q = 53$*, and the exponent is* $e = 17$*.*

- *Use the Extended Eulcidean algorithm to compute* $e^{-1} \bmod (p-1)(q-1)$*. Don't forget to mod out by* $(p-1)(q-1)$*.*
- *Encode the message "CMPT" using this cryptosystem. The numerical value of "CMPT" is 0313 1620.*

(You may use www.wolframalpha.com to do exponentiation modulo n)