Second Assignment

Mariano D'Angelo

4th April 2022

Task 1 — Big O Notation

Prove that $O(n^2) = an^2 + bn - c$, where a - is first 2 digits of your student code, b - is 3rd and 4th digit of your student code, c - last two digits of your student code.

Code 201752IVSB, then $a = 20$, $b = 17$, $c = 52$,
equation is $O(n^2) = 20n^2 + 17n - 52$

From theory we know that $f(n) \leq c \cdot g(n)$, so we get:

$20n^2 + 17n - 52 \leq c \cdot n^2$

To simplify our equation we can choose that $c = 21$. Now let's solve this:

$20n^2 + 17n - 52 \leq 21n^2$
$20n^2 - 21n^2 + 17n - 52 \leq 0$
$-n^2 + 17n - 52 \leq 0 \mid \cdot -1$
$n^2 - 17n + 52 \geq 0$

By taking the derivative of the quadratic formula we get:

$2n - 17 \geq 0$
$2n \geq 17$
$n = 8.5$

Meaning that the function starts to grow again after the value 8.5 is encountered.

By solving this quadratic formula equation we get the following values:

$n_1 = 13, n_2 = 4$, so $n < 4$ V $n > 13$

Meaning that the function is positive only when bigger than 4 or 13.

As a result we get — $c = 21, n = 14$

Task 2 — Complexity theory

Give an example of a *search* problem and corresponding *decision* problem, which was not discussed in the lectures.

Is $x \in \mathbb{Z}$ positive or negative?

Consider the corresponding verification function $V(x, y)$:

$$\begin{cases} 1 \text{ where } x = y + z \text{ and } (y \geq 0 \text{ and } z \geq 0) \text{ or } (+y > -|z| \text{ and viceversa}) \\ 0 \text{ if otherwise} \end{cases}$$

Search Problem (Summing): Given a positive x, find y such that $V(x, y) = 1$.

Decision Problem (Positiveness/Negativeness): Given x, decide if there is y such that $V(x, y) = 1$.

Task 3 — Block ciphers

Assume you are the agent of Mission Impossible. Top-level agents have decided that your agency will use AES-128 block cipher for its missions. You are given a task to choose a suitable encryption mode for the following mission scenarios:

1. Encryption of the agent's 6 digit identification number stored in the Super Secret Database (SSD)
2. Encryption of a document that will be sent via email.

Please, motivate your answer.