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.

1. In order to encrypt a 6 digit identification number I would use ECB. Even though it is not that safe when it comes to the encryption of multiple blocks (lack of diffusion), it can do well when it comes to the encryption of a single block. If we think of the 6 digit number as an integer it only occupies 4 bytes and we are encrypting with an 128 bit AES. Besides the lack of diffusion it has many positive sides, such as parallelizable encryption and decryption, and the possibility of random read.
2. In order to encrypt a document I would use CTR. This mode of encryption has many benefits, both encryption and decryption are parallelizable, random read is possible, faulty blocks affect only their current block. CTR uses a counter that is encrypted with the cipher text and increases with each block, so repeating ciphertext will not appear (good diffusion). No padding is used in the CTR mode (ciphertext is the same length as the plaintext) avoiding the padding oracle attack.

Task 4 — Modes of encryption

Alice wants to send a message m, encrypted with block cipher, to Bob. The message m is split into 4 blocks of equal length $m = m_0||m_1||m_2||m_3$ and encrypted using 3DES. However, a transmission error occurs (or malicious Carol got access to the channel) and one bit of the ciphertext c_1 changes its value.
Bob receives the ciphertexts, decrypts them and gets the following message $m' = m'_0||m'_1||m'_2||m'_3$. Please, explain to Bob how many bits (approximately) are expected to be wrong in each block m'_i if Alice used ECB and CBC modes.

Task 5 — Diffie-Hellman

Consider the Diffie-Hellman protocol with $\alpha = 3$ and $p = 673$. Alice chooses $A = 95$ and Bob chooses $B = 240$. Compute the messages that Alice and Bob send to each other and the final shared key.

Task 6 — Group theory

Do the following sets with defined operations form a group? Provide explanation.

- $\mathbb{Z}_{10}^{+}$ (*Integers modulo 10 under addition*)
- $\mathbb{Q}$ (*Rational numbers under multiplication*)
- $\mathbb{Z}_{37}^{-}$ (*Intergers under subtractions*)
- $(\mathbb{C} - 0, *)$ (*Complex numbers under multiplication*)