IBM3103 – Mathematical Methods for Biological and Medical Engineering

Fall 2021

Instructor: Carlos A. Sing Long
Teaching Assistant: Carlos Castillo

Assignment #1

March 26, 2021

Due on April 9, 2021

Problem #1: The nullspace (30pts)

Consider a collection $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ of n vectors in $\mathbb{R}^d$. To any vector $\boldsymbol{\alpha} \in \mathbb{R}^n$ we can associate the linear combination[1]

$$x(\boldsymbol{\alpha}) := \alpha_1 \boldsymbol{x}_1 + \ldots + \alpha_n \boldsymbol{x}_n.$$

Consider the following subset of $\mathbb{R}^n$

$$N := \{\boldsymbol{\alpha} \in \mathbb{R}^n : \; x(\boldsymbol{\alpha}) = \mathbf{0}\}.$$

(a) Show that N is a subspace of $\mathbb{R}^n$. In other words, that

$$\forall\, \boldsymbol{\alpha}, \boldsymbol{\beta} \in N,\, a, b \in \mathbb{R} : \; a\boldsymbol{\alpha} + b\boldsymbol{\beta} \in N.$$

(b) What can you say about the collection $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ if $N = \{\mathbf{0}\}$?

(c) What can you say about the collection $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ if N contains at least one non-zero vector?

Comment: If we define the matrix

$$\boldsymbol{X} := \begin{bmatrix} (x_1)_1 & \ldots & (x_n)_1 \\ \vdots & \ddots & \vdots \\ (x_1)_d & \vdots & (x_n)_d \end{bmatrix}$$

then the subspace N is called the **nullspace** of $\boldsymbol{X}$.

Problem #2: Polynomials and interpolation (30pts)

Consider d points $t_1, \ldots, t_d$ on the interval $[0, 1]$ given by

$$t_i = \frac{i-1}{d} \quad i \in \{1, \ldots, d\}.$$

You can think of these points as N instants between 0 and 1. Consider also the monomials

$$P_j(t) = t^j.$$

[1] Here we define the expression $x(\boldsymbol{\alpha})$ in terms of the right-hand side, so that there is no issue if you replace one by the other.

For example, $P_0(t) \equiv 1$, $P_1(t) = t$, $P_2(t) = t^2$, etc. Finally, consider the collection of vectors $\boldsymbol{p}_0, \ldots, \boldsymbol{p}_n$ in $\mathbb{R}^d$ defined as

$$\boldsymbol{p}_j := \begin{bmatrix} P_j(t_1) \\ \vdots \\ P_j(t_d) \end{bmatrix} = \begin{bmatrix} t_1^j \\ \vdots \\ t_d^j \end{bmatrix}.$$

In other words, the first component of $\boldsymbol{p}_j$ is the polynomial P_j evaluated at t_1, the second component is P_j evaluated at t_2, etc.

(a) Show that if $n < d$ the collection $\boldsymbol{p}_0, \ldots, \boldsymbol{p}_n$ is linearly independent. To show this, use the **fundamental theorem of calculus**: a polynomial of the form

$$Q(t) = a_0 + a_1 t + \ldots + a_n t^n$$

can be zero **at most** at n points **unless** $a_0 = \ldots = a_n = 0$.

(b) Let $d = 100$ and $n = 2$. Using `matplotlib` plot any linear combination of $\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2$ you want, indicating the scalars you used. What kind of polynomials do you get by taking linear combinations of $\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2$ (e.g. constant, linear, etc.)? Can you generalize this idea when $n > 2$?

(c) Let $d = 4$ and $n = 3$. Define the vector

$$\boldsymbol{f} = \begin{bmatrix} \cos(2\pi t_1) \\ \cos(2\pi t_2) \\ \cos(2\pi t_3) \\ \cos(2\pi t_4) \end{bmatrix}.$$

Using `numpy` find scalars $\alpha_0, \ldots, \alpha_3$ such that

$$\alpha_0 \boldsymbol{p}_0 + \ldots + \alpha_3 \boldsymbol{p}_3 = \boldsymbol{f}.$$

Furthermore, if $\alpha_0, \ldots, \alpha_3$ are the scalars you found, using `matplotlib` plot the functions

$$Q(t) = \alpha_0 + \alpha_1 t + \alpha_2 t^2 + \alpha_3 t^3 \quad \text{and} \quad f(t) = \cos(2\pi t)$$

on the same figure. What can you say about Q and f? **Comment:** Note Q and f coincide at $t_1, \ldots, t_4$. In this context, Q is an **interpolating polynomial** of f.

(d) Explain why there are some regions of the interval $[0, 1]$ where Q is a good approximation to f and others where it is not as good an approximation.

(e) **Bonus (+10pts):** Repeat (c) for $d = 6$ and $n = 5$. Is the polynomial Q closer to f?

Problem #3: Cipher (40pts)

In this question we will be using `Python` to solve a mystery. In the code `Example.py` that you can download from the course website, we have the systems `BlackBox1` and `BlackBox2`. Both represent an encryption system to be cracked. In the context of this question, that means that each system receives a **message**, called **plaintext**, represented by a vector of positive integers $\boldsymbol{\alpha} \in \mathbb{Z}_+^n$ and outputs an **encrypted message** $\boldsymbol{y} \in \mathbb{Z}_+^n$. The encryption procedure is represented by a linear combination with some collection of **keys** $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathbb{R}^n$

$$\boldsymbol{y} = \sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i.$$

Each black box has a different collection of keys $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

TABLE 1. Dictionary. Each letter is represented by a number.

Example: Suppose $n = 2$ and let's say our message is "HI" and the keys are "MA" and "TH." Then, we have

$$\left\{ \begin{bmatrix} M \\ A \end{bmatrix}, \begin{bmatrix} T \\ H \end{bmatrix} \right\} = \left\{ \begin{bmatrix} 13 \\ 1 \end{bmatrix}, \begin{bmatrix} 20 \\ 8 \end{bmatrix} \right\} \quad \text{and} \quad \boldsymbol{\alpha} = \begin{bmatrix} H \\ I \end{bmatrix} = \begin{bmatrix} 8 \\ 9 \end{bmatrix}.$$

Thus, the encrypted message is

$$\boldsymbol{y} = \sum_{i=1}^{2} \alpha_i \boldsymbol{x}_i = \begin{bmatrix} 284 \\ 80 \end{bmatrix}.$$

(a) Create a function `str2num` that transform a string to an array of numbers. Also, create another function `num2str` that does the opposite. Follow the rules of the dictionary in Table 1.

(b) Find a method to "crack" the keys $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathbb{R}^m$ of `BlackBox1` by sending a series of messages $\boldsymbol{\alpha}_k$. Remember, you **can not** send a zero as it is not present in the dictionary of Table 1. Which is the minimum amount of messages k necessary to obtain the keys? What is the message hidden in the keys?

(c) You have received the following mysterious message after passing through `BlackBox1`

$$\boldsymbol{y} = \begin{bmatrix} 1186 & 487 & 866 & 573 & 732 \end{bmatrix}^{\mathrm{t}}.$$

Which was the original message?

(d) Repeat question (b) but for `BlackBox2`. Is it possible to find the keys in this case? Justify your answer. Independent of the previous answer try to decipher the following encrypted message

$$\boldsymbol{y} = \begin{bmatrix} 295 & 331 & 627 & 368 \end{bmatrix}^{\mathrm{t}}.$$