Week 11 Tutorial Solutions

APSC 174 TAs

Week 11

Section 14

Question 1

For each of the following choices for the matrix A, establish whether or not A is invertible in the following two distinct ways:

(i) Check whether or not the column vectors of A are linearly independent.

(ii) Compute the determinant $\det(A)$ of A to see whether or not it is non-zero.

(a) - James

$$A = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}$$

Solution:

(i) First we check the linear independence of the columns: Let $\alpha, \beta \in \mathbb{R}$ and suppose that

$$\begin{aligned} & \alpha \cdot \begin{pmatrix} -1 \\ 2 \end{pmatrix} + \beta \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \iff & \begin{pmatrix} -\alpha + 2\beta \\ 2\alpha + \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \iff & \begin{cases} -\alpha + 2\beta & = 0 \\ 2\alpha + \beta & = 0 \end{cases} \\ \implies & \alpha = 2\beta \text{ and } \alpha = -\frac{1}{2}\beta \\ \implies & \alpha = \beta = 0 \end{aligned}$$

Thus the columns of A are LI.

(ii) As for the determinant, we will use the following basic formula:

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc.$$

Hence, for $\det A$ we get

$$\det A = (-1)(1) - (2)(2) = -5 \neq 0$$

so we may conclude that the columns of A are LI.

(n) - Jacob

$$A = \begin{pmatrix} 1 & 0 & 3 \\ 2 & 1 & 2 \\ 3 & 3 & 3 \end{pmatrix}$$

Solution:

(i) This can easily be checked using material taught in previous weeks to check linear independence. The final result is that the column vectors of A are linearly independent and hence A is invertible.

(ii) We want to choose a row to perform our determinant formula to that has the most zero entries. This is the first row.

$$\begin{aligned}
\det\left(\begin{pmatrix} 1 & 0 & 3 \\ 2 & 1 & 2 \\ 3 & 3 & 3 \end{pmatrix}\right) &= 1\det\left(\begin{pmatrix} 1 & 2 \\ 3 & 3 \end{pmatrix}\right) \qquad -0\det\left(\begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix}\right) + 3\det\left(\begin{pmatrix} 2 & 1 \\ 3 & 3 \end{pmatrix}\right) \\
&= 1(3 \cdot 1 - 2 \cdot 3) + 0 + 3(2 \cdot 3 - 3 \cdot 1) \\
&= 6.
\end{aligned}$$

(o) - Graeme

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Solution:

(i) Left as exercise.

(ii) We apply Laplace's expansion formula to the second column:

$$\begin{aligned}
\det\left(\begin{pmatrix} 3 & 2 & 1 \\ 2 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}\right) &= -2\det\left(\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\right) + 0 + 0 \\
&= -2(2 \cdot 1 - 1 \cdot 0) \\
&= -4.
\end{aligned}$$

(x) - Manfred

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 2 & -3 & 0 \\ 1 & 5 & -7 & 2 \end{pmatrix}$$

Solution:

(i) Linear Independence:

Let $v_1 = \begin{pmatrix}1\\1\\1\\1\end{pmatrix}, v_2 = \begin{pmatrix}0\\-1\\2\\5\end{pmatrix}, v_3 = \begin{pmatrix}0\\0\\-3\\-7\end{pmatrix}, v_4 = \begin{pmatrix}0\\0\\0\\2\end{pmatrix}$

We want to show if $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \alpha_4 v_4 = \mathbf{0}$

$\implies \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0.$

Solving each variable and using back-substitution, we obtain

$\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0$

Therefore, $\{v_1, v_2, v_3, v_4\}$ are linearly independent.

Therefore, A is invertible.

(ii) Computing Determinant:

$$\begin{aligned}\det(A) &= \det\begin{pmatrix}1 & 0 & 0 & 0\\1 & -1 & 0 & 0\\1 & 2 & -3 & 0\\1 & 5 & -7 & 2\end{pmatrix}\\ &= 1\cdot\det\begin{pmatrix}-1 & 0 & 0\\2 & -3 & 0\\5 & -7 & 2\end{pmatrix}\\ &= 1\cdot -1\cdot\det\begin{pmatrix}-3 & 0\\-7 & 2\end{pmatrix}\\ &= 1\cdot -1\cdot -3\cdot\det(2)\\ &= 1\cdot -1\cdot -3\cdot 2\\ &= 6\end{aligned}$$

(z) - Palmira

Given Matrix :

$$A = \begin{pmatrix}2 & 0 & 1 & 0\\0 & -2 & 5 & 0\\0 & 1 & 0 & 2\\1 & 1 & -1 & -1\end{pmatrix}$$

Solution:

(i) Checking Linear Independence:

$$\alpha\begin{pmatrix}2\\0\\0\\1\end{pmatrix} + \beta\begin{pmatrix}0\\-2\\1\\1\end{pmatrix} + \gamma\begin{pmatrix}1\\5\\0\\-1\end{pmatrix} + \lambda\begin{pmatrix}0\\0\\2\\-1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

Solving for each variable component wise gives:

$\alpha = 0, \beta = 0, \gamma = 0, \lambda = 0$

Hence, the column vecotrs of A are linearly independent

(ii) We apply Laplace's expansion formula to the first row to compute the determinant :

$$\det\left(\begin{pmatrix}2 & 0 & 1 & 0\\ 0 & -2 & 5 & 0\\ 0 & 1 & 0 & 2\\ 1 & 1 & -1 & -1\end{pmatrix}\right) = 2\det\left(\begin{pmatrix}-2 & 5 & 0\\ 1 & 0 & 2\\ 1 & -1 & -1\end{pmatrix}\right) + 0 + 1\det\left(\begin{pmatrix}0 & -2 & 0\\ 0 & 1 & 2\\ 1 & 1 & -1\end{pmatrix}\right) + 0$$

$$= 2\left(-2\det\left(\begin{pmatrix}0 & 2\\ -1 & -1\end{pmatrix}\right) - 5\det\left(\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\right)\right) + 2\det\left(\begin{pmatrix}0 & 2\\ 1 & -1\end{pmatrix}\right)$$

$$= 2\left(-2\cdot 2 - 5\cdot -3\right) + 2\cdot -2$$
$$= 18$$

Since $\det(A) \neq 0$, A is invertible.

Question 2

Refer to Message Scrambling portion of Section 13.

(a) - Siobhan

We are given the message M:

$$M = \begin{pmatrix}0 & 1 & 15 & 2 & 4 & 4 & 7 & 20\end{pmatrix} \quad (1)$$

Let us pick our scrambling matrix, A, at random, say:

$$A = \begin{pmatrix}5 & 2\\ 3 & 4\end{pmatrix} \quad (2)$$

Then we need to find the corresponding un-scrambling matrix, B, which is actually the inverse matrix of A.

$$B = A^{-1} = \frac{1}{det(A)}\begin{pmatrix}4 & -2\\ -3 & 5\end{pmatrix} \quad (3)$$

$$det(A) = det\begin{bmatrix}5 & 2\\ 3 & 4\end{bmatrix} = (5)(4) - (2)(3) = 14 \quad (4)$$

Thus the unscrambling matrix is:

$$B = \frac{1}{14}\begin{pmatrix}4 & -2\\ -3 & 5\end{pmatrix} = \begin{pmatrix}\frac{2}{7} & -\frac{1}{7}\\ -\frac{3}{14} & \frac{5}{14}\end{pmatrix} \quad (5)$$

Now we apply the scrambling matrix to the message in 1x2 chunks, first by multiplying each chunk by A to create the scrambled message, and then by multiplying each chunk by B to recreate the original message.

If M is split into the following 1x2 chunks:

$$\begin{pmatrix}0 & 1\end{pmatrix}, \begin{pmatrix}15 & 2\end{pmatrix}, \begin{pmatrix}4 & 4\end{pmatrix}, \begin{pmatrix}7 & 20\end{pmatrix} \quad (6)$$

Then when we apply A to each of them (multiplying on the right so that the internal dimensions line up: 1x2 with 2x2 gives 1x2):

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \end{pmatrix} \tag{7}$$

$$\begin{pmatrix} 15 & 2 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 81 & 38 \end{pmatrix} \tag{8}$$

$$\begin{pmatrix} 4 & 4 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 32 & 24 \end{pmatrix} \tag{9}$$

$$\begin{pmatrix} 7 & 20 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 95 & 94 \end{pmatrix} \tag{10}$$

So then the full encoded / scrambled message is:

$$M' = \begin{pmatrix} 3 & 4 & 81 & 38 & 32 & 24 & 95 & 94 \end{pmatrix} \tag{11}$$

Now let's de-scramble it! Un-encode it! We'll do this by multiplying our scrambled message, M', on the right by our descrambling matrix, B. In chunks:

$$\begin{pmatrix} 3 & 4 \end{pmatrix} \begin{pmatrix} \frac{2}{7} & -\frac{1}{7} \\ -\frac{3}{7} & \frac{5}{7} \end{pmatrix} = \begin{pmatrix} 0 & 1 \end{pmatrix} \tag{12}$$

$$\begin{pmatrix} 81 & 38 \end{pmatrix} \begin{pmatrix} \frac{2}{7} & -\frac{1}{7} \\ -\frac{3}{7} & \frac{5}{7} \end{pmatrix} = \begin{pmatrix} 15 & 2 \end{pmatrix} \tag{13}$$

$$\begin{pmatrix} 32 & 24 \end{pmatrix} \begin{pmatrix} \frac{2}{7} & -\frac{1}{7} \\ -\frac{3}{7} & \frac{5}{7} \end{pmatrix} = \begin{pmatrix} 4 & 4 \end{pmatrix} \tag{14}$$

$$\begin{pmatrix} 95 & 94 \end{pmatrix} \begin{pmatrix} \frac{2}{7} & -\frac{1}{7} \\ -\frac{3}{7} & \frac{5}{7} \end{pmatrix} = \begin{pmatrix} 7 & 20 \end{pmatrix} \tag{15}$$

So then the new message, M", is:

$$M'' = \begin{pmatrix} 0 & 1 & 15 & 2 & 4 & 4 & 7 & 20 \end{pmatrix} \tag{16}$$

Notice this is the original message, M! Why did this work? To each block of M, $M_{1\times 2block}$, we multiplied A and it's inverse B:

$$M''_{1\times 2block} = M'_{1\times 2block}B = (M_{1\times 2block}A)\,B = (M_{1\times 2block}A)\,A^{-1} = M_{1\times 2block}I = M_{1\times 2block} \tag{17}$$

Try this process again with a different choice of A, and you can check all of your matrix multiplication steps using Matlab :)

(c) - Taylor

We have the following message

$$M = \begin{pmatrix} 7 & 2 & 9 & 18 & 13 & 23 \end{pmatrix} \tag{18}$$

Now we wish to design a 3×3 scrambling matrix, A, and its corresponding unscrambling matrix B. From Problem (a), we know that we are going to need our scrambler A to be invertible. So while we are free to choose A at random, we have to be careful that it will in fact have a non-zero determinant (or linearly independent column vectors). Let's choose A as

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 0 & -1 & 2 \end{pmatrix} \tag{19}$$

Note that since A is lower triangular, its determinant is easily computed as

$$det(A) = a_{1,1}a_{2,2}a_{3,3} = (1)(3)(2) = 6 \neq 0$$

Now that we have a valid matrix A, we compute B from the requirement that $AB = I_{3\times 3}$.

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 0 & -1 & 2 \end{pmatrix} \begin{pmatrix} b_1 & b_4 & b_7 \\ b_2 & b_5 & b_8 \\ b_3 & b_6 & b_9 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

This gives a system of nine equations that can be solved without breaking too much of a sweat. I'll leave the grinding work as an exercise and just present the resultant B matrix. We find that

$$\begin{pmatrix} 1 & 0 & 0 \\ -2/3 & 1/3 & 0 \\ -1/3 & 1/6 & 1/2 \end{pmatrix}$$

Note: As a quick check to see if this answer makes sense, note that $det(B) = 1/6$, since B is again lower triangular. This is exactly the determinant we expect since we know that $AB = I$, and therefore

$$\begin{aligned} & det(AB) = det(I) \\ \Rightarrow\ & det(AB) = 1 \\ \Rightarrow\ & det(A)det(B) = 1 \\ \Rightarrow\ & det(B) = \frac{1}{det(A)} \end{aligned}$$

which is exactly what we observe. Now we can scramble and unscramble the message. To do this, we split the matrix into two 1×3 sub-matrices as follows

$$M = \begin{pmatrix} M_1 & \mid & M_2 \end{pmatrix} = \begin{pmatrix} 7 & 2 & 9 & \mid & 18 & 13 & 23 \end{pmatrix}$$

To scramble the first submatrix, M_1, we multiply by A *on the right*. The result is

$$M_1' = M_1 A = \begin{pmatrix} 11 & -3 & 18 \end{pmatrix}$$

We do the same for M_2 and find

$$M_2' = M_2 A = \begin{pmatrix} 44 & 16 & 46 \end{pmatrix}$$

So the scrambled message is then

$$M' = MA = \begin{pmatrix} 11 & -3 & 18 & 44 & 16 & 46 \end{pmatrix}$$

To unscramble it, we simply apply our unscrambler B *to the right as well*, just like we did in example (a) above. We do this in blocks again, this time using

$$M' = \begin{pmatrix} M_1' & \mid & M_2' \end{pmatrix} = \begin{pmatrix} 11 & -3 & 18 & \mid & 44 & 16 & 46 \end{pmatrix}$$

The unscrambled first block is then

$$M_1'' = M_1'B = \begin{pmatrix} 7 & 2 & 9 \end{pmatrix}$$

And the second block is

$$M_1'' = M_1'B = \begin{pmatrix} 18 & 13 & 23 \end{pmatrix}$$

Therefore the reconstructed message is

$$M'' = M'B = \begin{pmatrix} 7 & 2 & 9 & 18 & 13 & 23 \end{pmatrix}$$

We've recovered our original matrix! Just like in example (a), the reason is that the matrices A and B are actually inverses of each other, so mutliply first by A and then by B *on the same side* is just like multiplying by the identity matrix - nothing changes!