

The University of Melbourne
Department of Mathematics and Statistics
620-142 Mathematics B

Exam duration: Three hours

Reading time: 15 minutes

This paper has 8 pages.

The total number of marks allocated is 110.

Common Content: This examination paper contains questions in common with the paper for 620-122.

Authorized Materials: No materials are authorized. Calculators and mathematical tables are not permitted. Candidates are reminded that no written or printed material related to the subject may be brought into the examination. If you have any such material in your possession, you should immediately surrender it to an invigilator.

Instructions to Invigilators: One 14 page script book is to be given to each student initially. Students may retain this examination paper. No written or printed material related to the subject may be brought into the examination. No mathematical tables or calculators may be used.

Instructions to Students: This examination consists of 15 questions. All questions may be attempted.

However some question parts are harder (this is indicated with *, there are a total of 8 harder (*) marks) and it is not anticipated that all students will attempt these. Students who do attempt these are advised to complete the routine questions/question parts first.

The number of marks for each question is indicated on the examination paper. The total number of marks is 110. Use of calculators is neither allowed nor is it necessary for a successful completion of this examination paper.

Paper to be held by Baillieu Library: This paper may be reproduced and lodged with the Baillieu Library.

1. Working in \mathbb{Z}_{60} :

- (a) Find/write down $\gcd(17, 60)$.
- (b) Does 17 have a *multiplicative inverse* in \mathbb{Z}_{60} ? Explain.
- (c) Show that $17 \times 7 = -1$ in \mathbb{Z}_{60} .
- (d) Hence or otherwise find the *multiplicative inverse* of 17 in \mathbb{Z}_{60} .
- (e) * It is true that $\phi(60) = 16$.
Using Euler's Theorem (or otherwise) calculate 17^{17} in \mathbb{Z}_{60} .

[2 + 2 + 1 + 1 + 1* = 7 marks]

2. We are implementing the **RSA public key cryptosystem** with base $m = 77$.

- (a) Write 77 as the product of primes.
- (b) Calculate $n = \phi(m)$.
- (c) If the encryption key e is 17, find the decryption key d ,

$$\text{so that } a \xrightarrow{\text{encrypt}} a^e \xrightarrow{\text{decrypt}} (a^e)^d = a \text{ in } \mathbb{Z}_{77}.$$

- (d) Calculate 21^{31} in \mathbb{Z}_{77} .
Knowing $21^2 = 56$ and $56^2 = 21$ in \mathbb{Z}_{77} may help.
- (e) Explain (in no more than three sentences) what is meant by a cryptosystem being a *public key* cryptosystem.

[1 + 1 + 2 + 3 + 1 = 8 marks]

3. (a) Write down the value of a so that $0 \leq a < 25$ and $a = 15^2$ in \mathbb{Z}_{25} .

(b) * Show that $15^n = 0$ for all $n \geq 3$ in \mathbb{Z}_{25} .

(c) * Why isn't the RSA public key cryptosystem implementable with base $m = 25$?

[2 + 1* + 1* = 4 marks]

4. Let

$$A = \begin{bmatrix} 0 & 0 & 2 & -4 & 3 \\ 1 & -2 & 3 & -1 & 2 \\ 2 & -4 & 2 & 6 & -2 \\ 2 & -4 & 1 & 8 & 7 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & -2 & 0 & 5 & 0 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

In this question you may assume the fact that the matrix B is obtained from the matrix A by applying elementary row operations. Using this information, or otherwise, answer the following:

- What is the rank of A ?
- Write down a basis for the column space of A .
- Write down (or calculate) the dimension of the row space of A .
- Are the rows of A linearly independent? Explain your answer.
- Do the vectors $(0, 1, 2, 2)$, $(0, -2, -2, -4)$, $(2, 3, 2, 1)$, $(-4, -1, 6, 8)$, $(3, 2, -2, 7)$ span \mathbb{R}^4 ? Give a reason.
- Write $(-4, -1, 6, 8)$ as a linear combination of $(0, 1, 2, 2)$ and $(2, 3, 2, 1)$.
- Find a basis for the solution space of A .
- Let $T : \mathbb{R}^5 \rightarrow \mathbb{R}^4$ be the linear transformation with standard matrix A . Write down the rank of T ($=\dim(\text{Im}(T))$) and the nullity of T ($=\dim(\ker(T))$).

[1 + 2 + 1 + 2 + 2 + 1 + 2 + 2 = 13 marks]

5. (a) Let

$$W = \{(x, y) : x \times y \geq 0\} \subset \mathbb{R}^2$$

be the set of 2 dimensional real vectors whose coordinates are the same sign (or zero).

- Show that $(-1, -2)$ and $(2, 1)$ are both in W .
 - Show that W is **not** a subspace of \mathbb{R}^2 .
- (b) Consider the solution space $S = \{\mathbf{v} \in \mathbb{R}^4 : A\mathbf{v} = \mathbf{0}\}$ of the matrix

$$A = \begin{bmatrix} 3 & 2 & 1 & 3 \\ -1 & 2 & -1 & 2 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Show that S is a subspace of \mathbb{R}^4 .

- (c) * Consider \mathcal{F} the set of continuous functions with y -intercept 1, that is $\mathcal{F} = \{f : \mathbb{R} \rightarrow \mathbb{R} : f(0) = 1 \text{ and } f \text{ continuous}\}$.
Is this a subspace of the continuous functions $\mathbb{R} \rightarrow \mathbb{R}$? Explain.

[3 + 3 + 1* = 7 marks]

6. Consider the binary code \mathcal{C} with check matrix

$$B = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

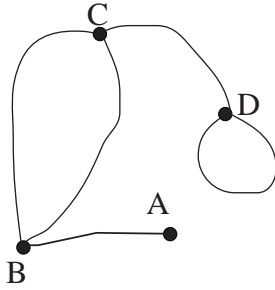
- (a) Which of the words 1001101, 1000001, 0010111 are codewords? Justify your answer (the calculations below may help).

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

- (b) What is the rank of B ?
- (c) The dimension of the code is 2.
Explain why this must be the case.
- (d) How many codewords does the code \mathcal{C} have?
- (e) Write down a basis for the code.
- (f) Hence write down all codewords for the code.
The code **can** correct 1 error.
- (g) Correct the word 0000111.
- (h) Explain why the code \mathcal{C} cannot correct two errors.
- (i) * Does there exist a set of 4 (distinct) columns of B that is linearly dependent? Explain.

[2 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1* = 10 marks]

7. Consider the following graph.



- (a) Write down the incidence matrix M for the graph, adopting the convention that row/col 1, row/col 2, row/col 3, row/col 4 correspond to vertices A, B, C, D respectively. Now

$$M^4 = \begin{bmatrix} 5 & 0 & 12 & 2 \\ 0 & 29 & 2 & 14 \\ 12 & 2 & 30 & 7 \\ 2 & 14 & 7 & 9 \end{bmatrix} \quad M^5 = \begin{bmatrix} 0 & 29 & 2 & 14 \\ 29 & 4 & 72 & 16 \\ 2 & 72 & 11 & 37 \\ 14 & 16 & 37 & 16 \end{bmatrix}.$$

- (b) Write down the number of 4 edge paths from B to B .
 (c) Write down the number of 5 edge paths from A to B .
 (d) * Explain *how* your answers to (ii) and (iii) are related and *why*.
 [2 + 1 + 1 + 2* = 6 marks]

8. (a) Find the line of best fit $y = a + bx$ to the data $(-1,6), (0,4), (1,0), (2,-1), (3,-4)$.
 (b) Sketch the line of best fit and include the data points on your graph.
 (c) With this line of best fit calculate the size of the error at $x = 0$.
 (d) Suppose you now try to fit a quadratic to the data. Write down the matrix A you would use in the formula

$$A^T A \bar{\mathbf{u}} = A^T \mathbf{y}$$

to solve the least squares problem. **Do not try to solve the problem.**

[5 + 2 + 1 + 1 = 9 marks]

9. For all $\mathbf{u} = (u_1, u_2, u_3)^T, \mathbf{v} = (v_1, v_2, v_3)^T$ in \mathbb{R}^3 we define

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} \rangle &= (u_1, u_2, u_3) \begin{bmatrix} 2 & -2 & 1 \\ -2 & 2 & 1 \\ 1 & 1 & -1 \end{bmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \\ &= \mathbf{u}^T A \mathbf{v} \\ \text{where } A &= \begin{bmatrix} 2 & -2 & 1 \\ -2 & 2 & 1 \\ 1 & 1 & -1 \end{bmatrix}. \end{aligned}$$

(a) Using $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^T A \mathbf{v}$ (or otherwise) show that

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle &= \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle, \\ \text{and } \langle \mathbf{u}, \alpha \mathbf{v} \rangle &= \alpha \langle \mathbf{u}, \mathbf{v} \rangle. \end{aligned}$$

(b) What property of the matrix A ensures $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$?

(c) Verify that $\mathbf{w} = \begin{bmatrix} 1 \\ 1 \\ -2 \end{bmatrix}$ is an *eigenvector* of A and find its *eigenvalue*.

(d) Using (iii) or otherwise find a vector \mathbf{u} such that $\langle \mathbf{u}, \mathbf{u} \rangle < 0$.

(e) Is \langle, \rangle an inner product? Explain your answer briefly. [3 + 1 + 2 + 1 + 1 = 8 marks]

10. (a) Use the Gram-Schmidt procedure to find an orthonormal basis for the subspace of \mathbb{R}^4 spanned by the vectors

$$(1, 0, 0, 0), (1, 1, 0, 0), (1, 1, 1, 1)$$

(Use the dot product on \mathbb{R}^4 as the inner product.)

(b) You may assume the columns of

$$B = \begin{bmatrix} \frac{2}{7} & \frac{3}{7} & \frac{6}{7} \\ \frac{6}{7} & \frac{2}{7} & -\frac{3}{7} \\ \frac{3}{7} & -\frac{6}{7} & \frac{2}{7} \end{bmatrix}$$

form an orthonormal basis.

Write down what would be output by the Matlab command:

$$\gg C = \mathbf{B}' \cdot \mathbf{B}$$

[5 + 1 = 6 marks]

11. Let $R : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be rotation by $\frac{\pi}{2}$ anticlockwise about the origin and let $S : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be reflection in the x -axis .

- (a) Write down the standard matrix representations for S and R .
- (b) Use part (a) to find the standard matrix representation for $S \circ R$ (R followed by S).
- (c) Draw the triangle T with corners at $(0, 0), (1, 0), (1, 1)$ in the xy -plane and on the same set of axes draw the image of this triangle T' after applying $S \circ R$.
- (d) Give a geometric interpretation of $S \circ R$.

[2 + 1 + 2 + 1 = 6 marks]

12. Consider the transformation $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by

$$T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 1 & 2 \\ -1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

- (a) Explain how we know by inspection that T is a linear transformation.

Let \mathcal{S} be the standard basis for \mathbb{R}^2 namely

$$\mathcal{S} = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}.$$

- (b) Write down $[T]_{\mathcal{S} \rightarrow \mathcal{S}}$ the standard matrix for T .

The set

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$$

is another basis for \mathbb{R}^2 .

- (c) Write down the transition matrix $P_{\mathcal{B} \rightarrow \mathcal{S}}$ from \mathcal{B} to \mathcal{S} .
- (d) Calculate the transition matrix $P_{\mathcal{S} \rightarrow \mathcal{B}}$ from \mathcal{S} to \mathcal{B} .
- (e) What is

$$P_{\mathcal{S} \rightarrow \mathcal{B}} [T]_{\mathcal{S} \rightarrow \mathcal{S}} P_{\mathcal{B} \rightarrow \mathcal{S}}$$

equal to?

- (f) Find $[T]_{\mathcal{B} \rightarrow \mathcal{B}}$.
- (g) If

$$[\mathbf{v}]_{\mathcal{B}} = \begin{bmatrix} 1 \\ 4 \end{bmatrix} \text{ find } [T(\mathbf{v})]_{\mathcal{B}}.$$

[1 + 1 + 1 + 2 + 1 + 2 + 1 = 9 marks]

13. (a) Calculate the *eigenvalues* of the matrix

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 5 \end{bmatrix}.$$

- (b) * Let $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ be eigenvectors for distinct eigenvalues.
What is the value of

$$\mathbf{u}_1 \cdot \mathbf{u}_2 + \mathbf{u}_2 \cdot \mathbf{u}_3 + \mathbf{u}_3 \cdot \mathbf{u}_1?$$

(Justify your answer.)

[4 + 1* = 5 marks]

14. (a) Show that

$$\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

are *eigenvectors* of

$$A = \begin{bmatrix} 1 & -1 & 1 \\ -4 & 4 & 2 \\ -2 & 2 & 4 \end{bmatrix}$$

and find their associated *eigenvalues*.

- (b) (i) Using 14(a) or otherwise write down an invertible matrix P and a diagonal matrix D so that

$$D = P^{-1}AP.$$

- (ii) Find a general *matrix* formula for A^n in terms of P, D and P^{-1} .

[5 + 2 + 1 = 8 marks]

15. The eigenvalues of $M = \begin{bmatrix} 2 & 1 & -1 \\ 1 & 3 & 2 \\ -1 & 2 & 3 \end{bmatrix}$ are 0, 3 and 5.

- (a) Find an eigenvector for the eigenvalue 0.

The vectors $\begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$ are eigenvectors for 3 and 5.

Notice that the matrix M is symmetric so that there is a matrix P so that $D = P^{-1}MP$ where D is diagonal.

- (b) (i) Write down suitable P and D .

- (ii) Write down an *orthogonal* matrix Q so that $D = Q^T M Q$.

[2 + 1 + 1 = 4 marks]