

The University of Melbourne
Department of Mathematics and Statistics
620-142 Mathematics B
Semester 2, 2007.

Reading time: 15 minutes.

Writing time: 3 hours.

This paper has 8 pages.

The total number of marks allocated is 120.

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

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.

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

The number of marks for each question is indicated on the examination paper. The total number of marks is 120. Use of calculators is not allowed.

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

1. (a) Using **Euclid's Algorithm** show that

$$\gcd(28, 11) = 1.$$

- (b) Using your working in (a) above (or otherwise) find the multiplicative inverse of 11 in \mathbb{Z}_{28} .
(c) Hence solve $11x = 3$ in \mathbb{Z}_{28} .
(d) What can be said about the existence of a multiplicative inverse of 7 in \mathbb{Z}_{77} ?

[7 marks]

2. Suppose the matrix A has eigenvector \mathbf{u} with eigenvalue λ that is

$$A\mathbf{u} = \lambda\mathbf{u}.$$

Using **mathematical induction** prove that A^n has eigenvector \mathbf{u} with eigenvalue λ^n that is

$$A^n\mathbf{u} = \lambda^n\mathbf{u}$$

for all integers $n \geq 1$.

[6 marks]

3. We are implementing the RSA public key cryptosystem with base $m = 58$.

- (a) Calculate $n = \phi(m)$.
(b) If the encryption key e is 23, find the decryption key d ,

$$\text{so that } a \xrightarrow{\text{encrypt}} a^e \xrightarrow{\text{decrypt}} (a^e)^d = a \text{ in } \mathbb{Z}_{58}.$$

Hint: d is in the set $\{8, 11, 53\}$. Justify your choice.

- (c) Use the decryption key d to decrypt the message '51' (that was encrypted with base $m = 58$ and encryption key $e = 23$).

Knowing $51 = -7, 7^2 = 49, 49^2 = 23$ and $23^2 = 7$ in \mathbb{Z}_{58} may help.

[8 marks]

4. In an implementation of the RSA public key cryptosystem:

- the base m (for \mathbb{Z}_m) and encryption key e are made public;
- the keys n and d are kept private.

- (a) Explain briefly how any 'message' $0 \leq a < m$ is encrypted and decrypted.
(b) Explain any special features of m and any relationships between m, e, n and d .
(c) In one or two sentences explain why with $m = p \times q$ where p and q are different 200 digit primes the public keys e and m **do not** reveal the private keys n and d .

[6 marks]

5. Let

$$A = \begin{bmatrix} 1 & 3 & -1 & 0 & 24 \\ 2 & 5 & 7 & -1 & 0 \\ -1 & -2 & -8 & 1 & 24 \\ 3 & -2 & 96 & 1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 0 & 26 & 0 & -6 \\ 0 & 1 & -9 & 0 & 10 \\ 0 & 0 & 0 & 1 & 38 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

In this question you may assume the fact that the matrix B was obtained using Matlab and the command: $B=\text{rref}(A)$.

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.
- Write down a basis for the row space of A .
- Do the vectors $(1, 2, -1, 3)$, $(3, 5, -2, -2)$, $(-1, 7, -8, 96)$, $(0, -1, 1, 1)$, $(24, 0, 24, 0)$ span \mathbb{R}^4 ? Give a reason.
- Write $(-1, 7, -8, 96)$ as a linear combination of $(1, 2, -1, 3)$ and $(3, 5, -2, -2)$.
- Find a basis for the solution space of A .
- Verify the rank/nullity theorem for the matrix A .

[13 marks]

6. (a) Complete points 1,2 and 3 missing from the following statement in your script books:

Subspace Theorem

IF $W \subseteq \mathbb{R}^n$ satisfies

1 ...

2 ...

3 ...

THEN

W is a subspace of \mathbb{R}^n .

(b) Let

$$P = \{(x, y, z) : x + y + z \leq 0\} \subset \mathbb{R}^3.$$

Show that P is NOT a subspace of \mathbb{R}^3 .

(c) Complete the following definition of a solution space of a matrix A in your script books:

$$\text{SolutionSpace}(A) = \{\mathbf{u} : A\mathbf{u} = \quad\}.$$

(d) Suppose A is an $m \times n$ matrix, using the subspace theorem show that the solution space of A is a subspace of \mathbb{R}^n .

[8 marks]

7. Consider the binary linear code \mathcal{C} with codewords $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\} = \{000000000, 101101101, 010110111, 111011010\}$, and check matrix

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

DO NOT show that \mathcal{C} is linear.

- (a) Using nearest neighbour decoding, correct the words:
 (i) 001101101;
 (ii) 001011010.
- (b) What is d_{\min} the minimum distance of the code \mathcal{C} ?
- (c) How many errors can the code \mathcal{C} :
 (i) correct;
 (i) detect.
- (d) Write down the dimension of the code \mathcal{C} .
- (e) Explain carefully why $\{101101101, 010110111\}$ forms a basis for the code \mathcal{C} .
- (f) Prove that H is a check matrix for the code \mathcal{C} . The Matlab output below may be useful for your justification.

```
>> H=[1 0 0 0 0 0 0 1 1;
      0 1 0 0 0 0 0 1 0;
      0 0 1 0 0 0 0 1 1;
      0 0 0 1 0 0 0 0 1;
      0 0 0 0 1 0 0 1 0;
      0 0 0 0 0 1 0 1 1;
      0 0 0 0 0 0 1 0 1];
```

```
>> c=[1 0 1 1 0 1 1 0 1;
      0 1 0 1 1 0 1 1 1];
```

```
>> mod(H*c',2)'
```

```
ans =
```

```
0 0 0 0 0 0 0
0 0 0 0 0 0 0
```

[10 marks]

8. (a) Find the line of best fit $y = a + bx$ to the 4 data points $\begin{array}{c|cccc} \mathbf{x} & -3 & -2 & 0 & 1 \\ \mathbf{y} & 9 & -7 & 3 & -1 \end{array}$
- (b) Suppose you now try to fit a quadratic $y = a + bx + cx^2$ 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.**

- (c) Giving a brief explanation, what least squares error would you expect for a cubic polynomial of best fit to this data?

[7 marks]

9. (a) The formula

$$\langle (a_1, a_2), (b_1, b_2) \rangle = 5a_1b_1 + 4a_1b_2 + 4a_2b_1 + 5a_2b_2 = \begin{bmatrix} a_1 & a_2 \end{bmatrix} \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

DOES define an inner product on \mathbb{R}^2 .

- (i) Write down all the properties $\langle \cdot, \cdot \rangle$ must satisfy to be an inner product on \mathbb{R}^2 .
DO NOT VERIFY THAT THESE PROPERTIES HOLD.
- (ii) Use this inner product to find $\|(1, -2)\|$ and $\langle (1, -2), (-2, 1) \rangle$.
- (b) Let us suppose that the following formula

$$\langle (u_1, u_2), (v_1, v_2) \rangle = u_1v_1 - 3u_1v_2 - 3u_2v_1 + u_2v_2$$

defines an inner product on \mathbb{R}^2 .

- (i) Find $\|(1, 1)\|^2$ using this formula.
- (ii) Does the formula in fact form an inner product? Explain your answer with reference to either the inner product axioms or $\|(1, 1)\|$.

[8 marks]

10. Let W be the span of the set

$$\mathcal{B} = \{(-2, 2, 1, 0), (-1, -2, 2, 0)\}.$$

- (a) Using the dot product and using the Gram Schmidt algorithm on \mathcal{B} or otherwise, find an orthonormal basis $\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2\}$ for W .
- (b) Find $\mathbf{p} = \text{Proj}_W(\mathbf{v})$, the orthogonal projection of $\mathbf{v} = (-3, 0, 3, 2)$ onto the subspace W .
- (c) Hence or otherwise, find an orthonormal basis for $W' = \langle \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}\} \rangle$ (the span of $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}\}$).

[8 marks]

11. Let $S : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ and $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be linear transformations on the plane with standard matrices

$$A_S = \begin{bmatrix} 1 & 6 \\ 0 & -2 \end{bmatrix} \text{ and } A_T = \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix} \text{ respectively. Let } \mathbf{x} = \begin{bmatrix} 2 \\ -1 \end{bmatrix}.$$

- (a) Calculate $\mathbf{w} = T(\mathbf{x})$.
 (b) Calculate $\mathbf{v} = S(\mathbf{w})$.
 (c) Calculate the standard matrix for $S \circ T$ (T followed by S).
 (d) Find the image with respect to $S \circ T$ of the vector \mathbf{x} .
 (e) What significance does the vector \mathbf{x} have for the standard matrix for $S \circ T$?

[8 marks]

12. (a) Find the eigenvalues and eigenvectors of the matrix

$$A = \begin{bmatrix} 5 & 6 \\ -2 & -2 \end{bmatrix}.$$

- (b) Describe geometrically what action the linear transformation

$$T(\mathbf{x}) = A\mathbf{x} \text{ has on the line } \left\langle \begin{bmatrix} 2 \\ -1 \end{bmatrix} \right\rangle.$$

[8 marks]

13. Consider the transformation $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by $T(\mathbf{x}) = A\mathbf{x}$ where

$$A = \begin{bmatrix} 5 & 6 \\ -2 & -2 \end{bmatrix}, \text{ that is } T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 5 & 6 \\ -2 & -2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Let \mathcal{S} and \mathcal{B} be the following bases for \mathbb{R}^2 :

$$\mathcal{S} = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}, \quad \mathcal{B} = \left\{ \begin{bmatrix} 3 \\ -2 \end{bmatrix}, \begin{bmatrix} 2 \\ -1 \end{bmatrix} \right\}.$$

- (a) Write down $[T]_{\mathcal{S} \rightarrow \mathcal{S}}$, the standard matrix for T .
 (b) Write down the transition matrix $P_{\mathcal{B} \rightarrow \mathcal{S}}$ from \mathcal{B} to \mathcal{S} .
 (c) Calculate the transition matrix $P_{\mathcal{S} \rightarrow \mathcal{B}}$ from \mathcal{S} to \mathcal{B} .
 (d) Hence or otherwise express $\mathbf{w} = \begin{bmatrix} -2 \\ -1 \end{bmatrix}$ as a linear combination of the vectors in the basis \mathcal{B} .
 (e) Calculate $[T]_{\mathcal{B} \rightarrow \mathcal{B}}$.
 (f) Find $[T(\mathbf{w})]_{\mathcal{B}}$.

[11 marks]

14. (a) Verify that the vectors

$$\begin{bmatrix} 4 \\ 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ -4 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

are eigenvectors of the matrix

$$A = \begin{bmatrix} 7 & 24 & 0 \\ 24 & -7 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and find their associated eigenvalues.

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

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

- (c) Write down an orthogonal matrix Q so that

$$D = Q^T A Q$$

(where D is the diagonal matrix above).

[9 marks]

15. Let A be an $n \times n$ real matrix.

- (a) Write down a condition (involving eigenvectors) for A to be diagonalizable.
(b) Write down a condition on A which will mean that A is orthogonally diagonalizable.
(c) Show that if A is orthogonally diagonalizable then the condition above in 15(b) must be satisfied.

[3 marks]