

Name: ..... Student ID: .....

UNSW SCHOOL OF MATHEMATICS AND STATISTICS

MATH3411 INFORMATION CODES AND CIPHERS

2018 S2

TEST 3

VERSION A

- Time Allowed: 45 minutes

For the multiple choice questions, **circle the correct answer**;  
each multiple choice question is worth **1 mark**.  
For the true/false and written answer questions, use extra paper.  
Staple everything together at the end.

1. A 2 symbol Markov source has transition matrix  $M = \begin{pmatrix} 0.75 & 0.4 \\ 0.25 & 0.6 \end{pmatrix}$  and equilibrium distribution  $\mathbf{p} = \frac{1}{13} \begin{pmatrix} 8 \\ 5 \end{pmatrix}$ . The (binary) Markov entropy  $H_M$  is approximately

(a) 0.716 (b) 0.961 (c) 0.891 (d) 0.873 (e) 0.910

2. A source  $S = \{s_1, s_2\}$  has probabilities  $P(s_1) = \frac{4}{5}$ ,  $P(s_2) = \frac{1}{5}$ . The second least likely codewords in the binary Shannon-Fano code for the third extension  $S^3$  have length

(a) 2 (b) 3 (c) 4 (d) 5 (e) 6

3. Consider a binary channel with source symbols  $\{a_1, a_2\}$  and output symbols  $\{b_1, b_2\}$  such that  $P(a_1) = \frac{3}{7}$ ,  $P(b_1 | a_1) = \frac{4}{5}$  and  $P(b_2 | a_2) = \frac{5}{8}$ . Recall the function

$$H(x) = -x \log_2 x - (1-x) \log_2 (1-x).$$

The noise entropy  $H(B | A)$  can be written as

(a)  $\frac{4}{7}H(\frac{4}{5}) + \frac{3}{7}H(\frac{5}{8})$  (b)  $\frac{4}{7}H(\frac{1}{5})$  (c)  $\frac{3}{7}H(\frac{1}{5}) + \frac{4}{7}H(\frac{3}{8})$  (d)  $\frac{3}{7}H(\frac{5}{8})$  (e)  $H(\frac{1}{5}) + H(\frac{3}{8})$

4. Use Euler's Theorem or otherwise to calculate  $10^{1001} \pmod{1001}$ .  
The answer is

(a) 1 (b) 10 (c) 100 (d) 101 (e) 901

5. For which of the following numbers  $a$  is  $n = 28$  a pseudo-prime to base  $a$ ?

(a) 3 (b) 9 (c) 12 (d) 18 (e) none of these

6. [5 marks] For each of the following, say whether the statement is true or false, giving a brief reason or showing your working. You will get  $\frac{1}{2}$  mark for a correct true/false answer, and if your true/false answer is correct, then you will get  $\frac{1}{2}$  mark for a good reason.

Begin each answer with the word “True” or “False”.

- i) There are 11 units in  $\mathbb{Z}_{22}$ .
- ii)  $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$  is a field.
- iii) When applied to  $n = 17$  with  $a = 3$ , Lucas’ test indicates that  $n$  is prime.
- iv) Given that 5 is a primitive element of  $\mathbb{Z}_{18}$ , 11 is also a primitive element of  $\mathbb{Z}_{18}$ .
- v) There are 60 primitive elements in  $\mathbb{U}_{125}$ .

7. [5 marks] Let  $\mathbb{F} = \mathbb{Z}_3[x]/\langle x^2 + x + 2 \rangle$ .

- (i) Express each nonzero element of  $\mathbb{F}$  as a power of a primitive element  $\alpha$  and as a linear combination over  $\mathbb{Z}_3$  of 1 and  $\alpha$ .
- (ii) Simplify  $\frac{\alpha^2 + 1}{\alpha^3 + \alpha^4}$ , giving your answer as a linear combination of 1 and  $\alpha$ .  
Show your working.
- (iii) Find the minimal polynomial of  $\alpha^2$ .

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Name: ..... Student ID: .....

UNSW SCHOOL OF MATHEMATICS AND STATISTICS

MATH3411 INFORMATION CODES AND CIPHERS

2018 S2

TEST 3

VERSION B

- Time Allowed: **45 minutes**

For the multiple choice questions, **circle the correct answer**;  
each multiple choice question is worth **1 mark**.  
For the true/false and written answer questions, use extra paper.  
Staple everything together at the end.

1. A 2 symbol Markov source has transition matrix  $M = \begin{pmatrix} 0.7 & 0.2 \\ 0.3 & 0.8 \end{pmatrix}$  and equilibrium distribution  $\mathbf{p} = \frac{1}{5} \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ . The (binary) Markov entropy  $H_M$  is approximately  
(a) 0.767    (b) 0.971    (c) 0.801    (d) 0.818    (e) 0.786
2. If a channel has input entropy  $H(A) = 0.93$ , output entropy  $H(B) = 0.76$  and mutual information  $I(A, B) = 0.56$ , then the joint entropy  $H(A, B)$  is approximately  
(a) 1.59    (b) 0.20    (c) 1.43    (d) 1.13    (e) 0.37
3. Use Euler's Theorem or otherwise to calculate  $5^{2018} \pmod{2018}$ .  
(Note that 1009 is prime. The answer is .....)  
(a) 1    (b) 5    (c) 25    (d) 125    (e) 625
4. Which of the following pairs consists of **two** primitive elements in  $\mathbb{Z}_{17}$ ?  
You may use the fact that 5 is a primitive element of  $\mathbb{Z}_{17}$ .  
(a) 2, 13    (b) 4, 11    (c) 6, 9    (d) 10, 6    (e) 13, 5
5. A source  $S = \{s_1, s_2\}$  has probabilities  $P(s_1) = \frac{5}{7}$ ,  $P(s_2) = \frac{2}{7}$ . The second most likely codewords in the ternary Shannon-Fano code for the third extension  $S^3$  have length  
(a) 2    (b) 3    (c) 4    (d) 5    (e) 6

6. [5 marks] For each of the following, say whether the statement is true or false, giving a brief reason or showing your working. You will get  $\frac{1}{2}$  mark for a correct true/false answer, and if your true/false answer is correct, then you will get  $\frac{1}{2}$  mark for a good reason.

Begin each answer with the word “True” or “False”.

- i) There are 24 units in  $\mathbb{Z}_{48}$ .
- ii) The polynomial  $m(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$  is irreducible.
- iii) There are 8 primitive elements in  $\mathbb{U}_{31}$ .
- iv)  $n = 65$  is a pseudo-prime to base 5.
- v) When applied to  $n = 61$  with  $a = 3$ , Lucas’ test indicates that  $n$  is prime.

7. [5 marks] Let  $\mathbb{F} = \mathbb{Z}_3[x]/\langle x^2 + 2x + 2 \rangle$ .

- (i) Express all nonzero elements of  $\mathbb{F}$  as a power of a primitive element  $\alpha$  and as a linear combination over  $\mathbb{Z}_3$  of 1,  $\alpha$ .
- (ii) Solve the set of linear equations

$$\begin{pmatrix} \alpha^4 & \alpha^5 \\ \alpha^2 & \alpha^7 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ \alpha^3 \end{pmatrix}$$

in  $\mathbb{F}$ .

- (iii) Find the minimal polynomial of  $\alpha^5$ .  
Show your working

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder