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

UNSW School of Mathematics and Statistics

MATH3411 Information Codes and Ciphers

2014 S2 **TEST 2** **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. If arithmetic coding with source symbols s_1, s_2 and the stop symbol • corresponding to the intervals $[0, 0.4)$, $[0.4, 0.9)$ and $[0.9, 1)$ is used, then the message 0.69 decodes as

(a) $s_2 s_1 \bullet$ (b) $s_1 s_1 \bullet$ (c) $s_2 s_1 s_1 \bullet$ (d) $s_1 s_1 s_2 \bullet$ (e) $s_2 s_2 s_1 \bullet$

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

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

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

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

and note that $H(x) = H(1 - x)$. The noise entropy $H(B \mid A)$ 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. Using Euler's Theorem or otherwise, calculate $3^{940} \pmod{2014}$.
(NB: 1007 is not prime.) The answer is

(a) 1 (b) 3 (c) 9 (d) 27 (e) 81

5. For which of the following numbers a is $n = 15$ a pseudoprime to base a?

(a) 2 (b) 3 (c) 4 (d) 5 (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) The LZ78 algorithm decodes the message $(0, a)(1, a)(1, b)(2, a)(2, b)(4, a)$ as $aaaabaaaaabaaaa$.

ii) For a 3-symbol source $S = \{s_1, s_2, s_3\}$ with probabilities $p_1 = 4/7$, $p_2 = 2/7$, $p_3 = 1/7$, it is possible to find a binary encoding of some extension S^n with average word length per original source symbol less than 1.28.

iii) When using Fermat factorisation to factor $n = 6283$ as a product $n = ab$ where $2 \le a < b$, the linear combination $a + 2b$ equals 271.

iv) For symbols s_1, s_2, s_3, s_4 with probabilities $0.50,\ 0.25,\ 0.13,\ 0.12$ respectively, the binary Shannon-Fano encoding 0101110 encodes the string of symbols $s_1 s_2 s_4$.

v) There are 6 primitive elements in the field GF(27).

7. [**5 marks**] Let $\mathbb{F} = \mathbb{Z}_2(\alpha)$ where α is a root of the polynomial $x^3 + x + 1 \in \mathbb{Z}_2[x]$.

(i) Express all nonzero elements of $\mathbb{F}$ as powers of α and as linear combinations over $\mathbb{Z}_2$ of 1, α, and α^2.

(ii) Find the value of $k \in \{1, \ldots, 7\}$ for which $(\alpha + 1)^k = \alpha^2 + \alpha + 1$.

(iii) Find the minimal polynomial of α^3.
Show your working.

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

UNSW SCHOOL OF MATHEMATICS AND STATISTICS

MATH3411 INFORMATION CODES AND CIPHERS

2014 S2 **TEST 2** **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. If arithmetic coding with source symbols s_1, s_2 and the stop symbol $\bullet$ corresponding to the intervals $[0, 0.4)$, $[0.4, 0.9)$ and $[0.9, 1)$ is used, then the message 0.35 decodes as

(a) $s_1s_2\bullet$ (b) $s_2s_1\bullet$ (c) $s_2s_2s_1\bullet$ (d) $s_1s_1s_2\bullet$ (e) $s_2s_1s_1\bullet$

2. 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) 0.712 (b) 0.786 (c) 0.802 (d) 0.818 (e) 0.971

3. Consider a binary channel with source symbols $\{a_1, a_2\}$ and output symbols $\{b_1, b_2\}$ such that $P(a_1) = \frac{1}{5}$, $P(b_1 \mid a_1) = \frac{4}{5}$ and $P(b_2 \mid a_2) = \frac{5}{8}$. Recall the function

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

and note that $H(x) = H(1 - x)$. The noise entropy $H(B \mid A)$ can be written as

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

4. Using Euler's Theorem or otherwise, calculate $2^{2014} \pmod{123}$. The answer is

(a) 1 (b) 2 (c) 4 (d) 25 (e) 107

5. Which of the following pairs consists of **two** primitive elements in $\mathbb{Z}_{17}$?
You may use the fact that 3 is a primitive element of $\mathbb{Z}_{17}$.

(a) 5, 9 (b) 5, 10 (c) 9, 10 (d) 9, 12 (e) 12, 13

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) The LZ78 algorithm decodes the message $(0, a)(1, a)(0, b)(2, a)(2, b)(3, a)$ as $aaabaaaaabba$.

ii) For a 3-symbol source $S = \{s_1, s_2, s_3\}$ with probabilities $p_1 = 5/11$, $p_2 = 4/11$, $p_3 = 2/11$ it is possible to find a binary encoding of some extension S^n with average word length per original source symbol less than 1.5.

iii) When using Fermat factorisation to factor $n = 6283$ as a product $n = ab$ where $2 \leq a < b$, the linear combination $2a + b$ equals 215.

iv) For symbols s_1, s_2, s_3, s_4 with probabilities $0.5,\ 0.2,\ 0.2,\ 0.1$ respectively, the binary Shannon-Fano encoding 01001100 encodes the string of symbols $s_1 s_2 s_4$.

v) The number 3 is one of the pseudo-random numbers generated by the linear congruential $x_{i+1} \equiv 2x_i + 5 \pmod{17}$, seeded with $x_0 = 1$.

7. [**5 marks**] Let $\mathbb{F} = \mathbb{Z}_2(\alpha)$ where α is a root of the polynomial $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$.

(i) Express all nonzero elements of $\mathbb{F}$ as powers of α and as linear combinations over $\mathbb{Z}_2$ of 1, α, and α^2.

(ii) Simplify $\dfrac{\alpha^2 + 1}{\alpha^3 + \alpha^4}$, giving your answer as a linear combination of 1, α and α^2. Show your working.

(iii) Find the minimal polynomial of α^5.
Show your working.