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

UNSW School of Mathematics and Statistics

MATH3411 Information Codes and Ciphers

2015 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 a, b 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 $bba\bullet$ could encode as

(a) 0.60 (b) 0.64 (c) 0.69 (d) 0.74 (e) 0.80

2. A 2-symbol Markov source has transition matrix $M = \begin{pmatrix} 0.5 & 0.7 \\ 0.5 & 0.3 \end{pmatrix}$ and equilibrium distribution $\mathbf{p} = \frac{1}{12}\begin{pmatrix} 7 \\ 5 \end{pmatrix}$. The (binary) Markov entropy H_M is approximately

(a) 0.931 (b) 0.941 (c) 0.951 (d) 0.967 (e) 0.980

3. Consider a binary channel with source symbols $\{a_1, a_2\}$ and output symbols $\{b_1, b_2\}$ such that $P(a_1) = \frac{1}{4}$, $P(b_1 \mid a_1) = \frac{4}{7}$ and $P(b_2 \mid a_2) = \frac{3}{8}$. 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) $\frac{1}{4}H(\frac{4}{7}) + \frac{3}{4}H(\frac{5}{8})$ (b) $\frac{3}{8}H(\frac{1}{4}) + \frac{4}{7}H(\frac{3}{4})$ (c) $\frac{4}{7}H(\frac{1}{4}) + \frac{3}{8}H(\frac{3}{4})$ (d) $\frac{3}{4}H(\frac{4}{7}) + \frac{1}{4}H(\frac{3}{8})$ (e) $\frac{3}{8}H(\frac{3}{4}) + \frac{4}{7}H(\frac{1}{4})$

4. Using Euler's Theorem or otherwise, calculate $2^{2015} \pmod{125}$.
The answer is

(a) 2 (b) 6 (c) 9 (d) 18 (e) 36

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

(a) 2 (b) 3 (c) 7 (d) 9 (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 encodes the message *aaaabaaaaabaaaa* as

$$(0, a)(1, a)(1, b)(2, a)(2, b)(4, a)\,.$$

ii) For a 3-symbol source $S = \{s_1, s_2, s_3\}$ with probabilities $p_1 = 4/9$, $p_2 = 2/9$, $p_3 = 1/3$ 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 $n = 1891$ as a product $n = ab$ where $2 \leq a < b$, the linear combination $2a - b$ equals 1.

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

v) There are 16 primitive elements in the field GF(49).

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) Solve the set of linear equations

$$\begin{pmatrix} \alpha^3 & \alpha^5 \\ \alpha^2 & \alpha^3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha \\ \alpha^6 \end{pmatrix}$$

in $\mathbb{F}$.

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

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

UNSW School of Mathematics and Statistics

MATH3411 Information Codes and Ciphers

2015 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 a, b 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) $aa\bullet$ (b) $aab\bullet$ (c) $ab\bullet$ (d) $ba\bullet$ (e) $baa\bullet$

2. A 2-symbol Markov source has transition matrix $M = \begin{pmatrix} 0.8 & 0.5 \\ 0.2 & 0.5 \end{pmatrix}$ and equilibrium distribution $\mathbf{p} = \frac{1}{7}\begin{pmatrix} 5 \\ 2 \end{pmatrix}$. The (binary) Markov entropy H_M is approximately

(a) 0.801 (b) 0.851 (c) 0.863 (d) 0.887 (e) 0.921

3. Consider a binary channel with source symbols $\{a_1, a_2\}$ and output symbols $\{b_1, b_2\}$ such that $P(a_1) = \frac{5}{6}$, $P(b_1 \mid a_1) = \frac{3}{5}$ and $P(b_2 \mid a_2) = \frac{2}{7}$. 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) $\frac{2}{7}H(\frac{5}{6}) + \frac{3}{5}H(\frac{1}{6})$ (b) $\frac{1}{6}H(\frac{3}{5}) + \frac{5}{6}H(\frac{2}{7})$ (c) $\frac{5}{6}H(\frac{3}{5}) + \frac{1}{6}H(\frac{5}{7})$ (d) $\frac{3}{5}H(\frac{5}{6}) + \frac{2}{7}H(\frac{1}{6})$ (e) $\frac{2}{7}H(\frac{1}{6}) + \frac{3}{5}H(\frac{5}{6})$

4. Using Euler's Theorem or otherwise, calculate $3^{2015} \pmod{125}$. The answer is

(a) 1 (b) 3 (c) 5 (d) 25 (e) 32

5. For which of the following numbers a is $n = 24$ a pseudoprime to base a?

(a) 2 (b) 3 (c) 5 (d) 7 (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 encodes the message *aaabaaaaabba* as

$$(0,a)(1,a)(0,b)(2,a)(2,b)(3,a)\,.$$

ii) For a 3-symbol source $S = \{s_1, s_2, s_3\}$ with probabilities $p_1 = 1/2$, $p_2 = 1/6$, $p_3 = 1/3$, 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 $n = 2257$ as a product $n = ab$ where $2 \leq a < b$, the linear combination $2a - b$ equals 1.

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

v) Given that 3 is a primitive element of $\mathbb{Z}_{19}$, then 15 is also a primitive element.

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) Solve the set of linear equations

$$\begin{pmatrix} \alpha^2 & \alpha^5 \\ \alpha^4 & \alpha^6 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ 1 \end{pmatrix}$$

in $\mathbb{F}$.

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