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

UNSW SCHOOL OF MATHEMATICS AND STATISTICS

MATH3411 INFORMATION CODES AND CIPHERS

2011 S2 **TEST 2** **VERSION A**

- Time Allowed: **45 minutes**

For the multiple choice questions, **circle the correct answer**; each multiple choice question is worth 2 marks.
For the true/false and written answer questions, use extra paper.
Staple everything together at the end.

1. Using the LZ78 algorithm a message is encoded as $(0, a)(1, b)(2, a)(2, b)$. The message is

(a) $aababbaba$ (b) $abbbbabbb$ (c) $abbaaaabb$

(d) $aababaabb$ (e) $aababbabb$

2. Let $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$, so that $H'(x) = \log_2(x^{-1} - 1)$. An asymmetric binary channel with input $A = \{a_1, a_2\}$ and output $B = \{b_1, b_2\}$ has noise entropy $H(B \mid A) = 0.7p + 0.2$ in bits with $H(B) = H(0.1 + 0.4p)$ in bits and $p = P(a_1)$. The channel capacity is achieved when p has the value approximately

(a) 0.23 (b) 0.32 (c) 0.76 (d) 0.38 (e) 0.55

3. Let $f(x) = x^4 + 2x^2 + 2$ and $g(x) = x^2 + 3x + 2$ be polynomials in $\mathbb{Z}_5[x]$. The remainder when $f(x)$ is divided by $g(x)$ in $\mathbb{Z}_5[x]$ is

(a) 2 (b) $x^2 + 2x + 4$ (c) $3x$ (d) $x + 1$ (e) $4x + 4$

4. Applying the Pollard-ρ method with $x_0 = 3$ and $x_i = x_{i-1}^2 + 1 \pmod{n}$ for $i > 0$ finds which factor of $n = 1105 = 5 \times 13 \times 17$ first?

(a) 5 (b) 13 (c) 17 (d) 65 (e) 85

5. Suppose that the linear congruential pseudorandom number generator

$$x_{i+1} \equiv 3x_i + 5 \pmod{7}$$

is given the seed $x_0 = 3$. Then x_5 equals

(a) 0 (b) 1 (c) 2 (d) 3 (e) 4

6. **[10 marks]** For each of the following, say whether the statement is true or false and giving a brief reason or showing your working. You will get one mark for a correct true/false answer, and if your true/false answer is correct then you will get one mark for a good reason.

Begin each answer with the word "true" or "false".

i) If a source S has binary entropy 2.5, then a Huffman coding of the fourth extension must have average length per original source symbol less than 2.8 .

ii) For a noisy binary channel the entropy of the output is always larger than the entropy of the input.

iii) $5^{2011} \equiv 12 \pmod{13}$.

iv) There are 42 primitive elements in the field GF(49).

v) In the field $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$, if α is a root of $x^3 + x + 1$ then $\alpha^6 = \alpha^2 + 1$.

7. **[10 marks]** A source S has 5 symbols $s_1, s_2, \ldots, s_5$ with probabilities

$$\frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{2}{15}, \frac{1}{12}$$

respectively.

i) Find the entropy of S in **bits**.

ii) Find a **ternary** (radix 3) Shannon-Fano code for S and calculate its expected codeword length.

iii) A **binary** Shannon-Fano code is constructed for S^3. (**Do not** try to find it.) Find the lengths of the two shortest codewords in this code.

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

UNSW School of Mathematics and Statistics

MATH3411 Information Codes and Ciphers

2011 S2 **TEST 2** **VERSION B**

- Time Allowed: **45 minutes**

For the multiple choice questions, **circle the correct answer**; each multiple choice question is worth 2 marks. For the true/false and written answer questions, use extra paper. Staple everything together at the end.

1. Using the LZ78 algorithm a message is encoded as $(0,a)(1,b)(0,c)(2,a)(4,c)(5,b)$. What is the last dictionary entry after decoding?

(a) $abacb$ (b) $abcab$ (c) $abac$ (d) $acbcb$ (e) $abbcb$

2. Let $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$, so that $H'(x) = \log_2(x^{-1} - 1)$. An asymmetric binary channel with input $A = \{a_1, a_2\}$ and output $B = \{b_1, b_2\}$ has noise entropy $H(B\,|\,A) = 0.8p + 0.3$ in bits with $H(B) = H(0.1 + 0.5p)$ in bits where $p = P(a_1)$. The channel capacity is achieved when p has the value approximately

(a) 0.25 (b) 0.53 (c) 0.30 (d) 0.36 (e) 0.62

3. Let $f(x) = x^4 + 2x^3 + x$ and $g(x) = x^2 + x + 2$ be polynomials in $\mathbb{Z}_5[x]$. The remainder when $f(x)$ is divided by $g(x)$ in $\mathbb{Z}_5[x]$ is

(a) $2x$ (b) $x+3$ (c) x^2+x+2 (d) $2x+1$ (e) $2x+4$

4. Applying the Pollard-ρ method with $x_0 = 3$ and $x_i = x_{i-1}^2 + 1 \pmod{n}$ for $i > 0$ finds which factor of $n = 1001 = 7 \times 11 \times 13$ first?

(a) 7 (b) 11 (c) 13 (d) 91 (e) 143

5. Suppose that the linear congruential pseudorandom number generator

$$x_{i+1} \equiv 3x_i + 4 \pmod{7}$$

is given the seed $x_0 = 1$. Given that the period of the generator is 6, which of these members of $\mathbb{Z}_7$ is **not** generated:

(a) 0 (b) 2 (c) 3 (d) 4 (e) 5

6. [**10 marks**] For each of the following, say whether the statement is true or false and giving a brief reason or showing your working. You will get one mark for a correct true/false answer, and if your true/false answer is correct then you will get one mark for a good reason.

Begin each answer with the word "true" or "false".

i) If a source S has binary entropy 2.4, then the Shannon-Fano coding of the fifth extension must have average length per original source symbol less than 2.7 .

ii) For a noisy channel the entropy of the input can be larger than the entropy of the output.

iii) $2^{2011} \equiv 11 \pmod{13}$.

iv) There are 32 primitive elements in the field GF(121).

v) In the field $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle$, if α is a root of $x^3 + x^2 + 1$ then $\alpha^6 = \alpha^2 + 1$.

7. [**10 marks**] A source S has 5 symbols $s_1, s_2, \ldots, s_5$ with probabilities

$$\frac{2}{5}, \quad \frac{1}{4}, \quad \frac{1}{6}, \quad \frac{1}{10}, \quad \frac{1}{12}$$

respectively.

i) Find the entropy of S in **bits**.

ii) Find a **ternary** (radix 3) Shannon-Fano code for S and calculate its expected codeword length.

iii) A **binary** Shannon-Fano code is constructed for S^2. (**Do not** try to find it.) Find the lengths of the two longest codewords in this code.