MATH3411 INFORMATION, CODES & CIPHERS

Test 2, Session 2 2013, SOLUTIONS

Version A

Multiple choice: **a**, **e**, **a**, **d**, **e**
True/False: **T**, **T**, **F**, **T**, **F** .

1. **(a)**

2. **(e)**: $M_H = \frac{2}{3}H(0.8) + \frac{1}{3}H(0.4) \approx 0.805$.

3. **(a)**: $I(A,B) = H(B) - H(B|A) = H(0.3+0.5p) - (0.4p + 0.6)$. Differentiating $I(A,B)$ with respect to p and setting $I'(A,B) = 0$ gives

$$0.5\log_2((0.3+0.5p)^{-1} - 1) = 0.4\,,$$

so $(0.3+0.5p)^{-1} = 2^{0.8} + 1 \approx 2.74$. Solving this gives $p \approx 0.13$.

4. **(d)**: $\phi(2013) = \phi(3 \times 11 \times 61) = \phi(3)\phi(11)\phi(61) = 2 \times 10 \times 60 = 1200$, so $2^{1203} \equiv 2^{1200+3} \equiv 8$ in $\mathbb{Z}_{2013}$.

5. **(e)**

6. (i) **True**: We wish to decode the number 0.55 :

code number rescaled	in interval	decoded symbol
0.55	$[0.3, 0.7)$	b
$(0.55-0.3)/.4 = 0.625$	$[0.3, 0.7)$	b
$(0.625-0.3)/.4 = 0.8125$	$[0.7, 1)$	$\bullet$

The decoded message is then $bb\bullet$.

(ii) **True**: The binary entropy is 0.722 and by Shannon's Theorem, we can get arbitrarily close to this.

(iii) **False**: $t = \lceil\sqrt{1333}\rceil = 37$ gives $s^2 = t^2 - n = 36 = 6^2$ which is square, so $a + b = (s+t) + (t-s) = 2t = 74$.

(iv) **True**: The second smallest symbol probability in S^3 is $\frac{4}{125}$, and $\frac{125}{4} = 31.25 < 32 = 2^5$, so the second longest codeword length is $\ell = 5$.

(v) **False**: The numbers x_i are 1, 6, 4, 7, 8 .

7. (i) Here, we have that $\alpha^2 = -1 = 2$.

γ^1	$= \alpha + 1$	γ^5	$= 2\alpha + 2$
γ^2	$= 2\alpha$	γ^6	$= \alpha$
γ^3	$= 2\alpha + 1$	γ^7	$= \alpha + 2$
γ^4	$= 2$	γ^8	$= 1$

(ii) The element γ is primitive, so all of the primitive elements of $\mathbb{F}$ are given by γ^i where $\gcd(i, 8) = 1$; that all of the 4 elements

$$\gamma^1 = \alpha + 1\,,\ \gamma^3 = 2\alpha + 1\,,\ \gamma^5 = 2\alpha + 2\,,\ \gamma^7 = \alpha + 2$$

(iii) $\alpha^{-1} = (\gamma^6)^{-1} = \gamma^2 = 2\alpha$.

(iv) $\dfrac{\gamma^7 + \alpha}{\gamma^4 + \gamma} = \dfrac{2\alpha + 2}{\alpha} = 2 + \dfrac{2}{\alpha} = 2 + 2(2\alpha) = 2 + \alpha$

Version B

Multiple choice: **c**, **d**, **a**, **d**, **c**
True/False: **F**, **F**, **T**, **T**, **T**.

1. **(c)**

2. **(d)**: $M_H = \frac{1}{3}H(0.8) + \frac{2}{3}H(0.4) \approx 0.888$.

3. **(a)**: $I(A,B) = H(B) - H(B|A) = H(0.2 + 0.7p) - (0.4p + 0.7)$.
Differentiating $I(A,B)$ with respect to p and setting $I'(A,B) = 0$ gives

$$0.7 \log_2((0.2 + 0.7p)^{-1} - 1) = 0.4\,,$$

so $(0.2 + 0.7p)^{-1} = 2^{\frac{4}{7}} + 1 \approx 2.49$. Solving this gives $p \approx 0.29$.

4. **(d)**: $\phi(2013) = \phi(3 \times 11 \times 61) = \phi(3)\phi(11)\phi(61) = 2 \times 10 \times 60 = 1200$,
so $5^{1203} = 5^{1200}5^3 = 125$ in $\mathbb{Z}_{2013}$.

5. **(c)** $4^{14} \equiv 1 \pmod{15}$

6. (i) **False**: We wish to decode the number 0.55.

code number rescaled	in interval	decoded symbol
0.55	$[0.3, 0.7)$	b
$(0.55 - 0.3)/.4 = 0.625$	$[0.3, 0.7)$	b
$(0.625 - 0.3)/.4 = 0.8125$	$[0.7, 1)$	•

The decoded message is then $bb\bullet$.

(ii) **False**: The binary entropy is 0.81 which is the lower bound on average codeword lengths.

(iii) **True**: $t = \lceil\sqrt{1333}\rceil = 37$ gives $s^2 = t^2 - n = 36 = 6^2$ which is square, so $a + b = (s + t) + (t - s) = 2t = 74$.

(iv) **True**: The second largest symbol probability in S^3 is $\frac{16}{125}$, and $\frac{125}{16} = 7.8125 < 8 = 2^3$, so the second shortest codeword length is $\ell = 3$.

(v) **True**: The numbers x_i are 1, 6, 4, 7, 8.

7. (i) Here, we have that $\alpha^2 = 2\alpha + 1$.

i	0	1	2	3	4	5	6	7	8
α^i	1	α	$2\alpha+1$	$2\alpha+2$	2	2α	$\alpha+2$	$\alpha+1$	1

(ii) The element α is primitive, so all of the primitive elements of $\mathbb{F}$ are given by α^i where $\gcd(i, 8) = 1$; that is all of the 4 elements

$$\alpha^1 = \alpha\,,\ \alpha^3 = 2\alpha + 2\,,\ \alpha^5 = 2\alpha\,,\ \alpha^7 = \alpha + 1$$

(iii) $(2\alpha + 1)^{-1} = (\alpha^2)^{-1} = \alpha^6 = \alpha + 2.$

(iv) $\dfrac{\alpha^2 + 1}{\alpha^3 + \alpha^4} = \dfrac{2\alpha + 2}{2\alpha + 1} = \dfrac{\alpha^3}{\alpha^2} = \alpha$