MATH3411 INFORMATION, CODES & CIPHERS

Test 2 Session 2 2017 SOLUTIONS

Version A

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

1. **(e)**: 1. b, 2. a, 3. aa, 4. aab, 5. aaa

2. **(b)**: $H_M = \frac{1}{4}H(0.7) + \frac{3}{4}H(0.4) \approx 0.904$

3. **(a)**: $I(A,B) = H(B) - H(B|A) = H(0.2+0.7p) - (0.4p+0.1)$,
so $\frac{d}{dp}I(A,B) = 0.7\log_2(\frac{1}{0.2+0.7p} - 1) - 0.4$.
Setting $\frac{d}{dp}I(A,B) = 0$ yields $p = \frac{1}{0.7}\left((2^{\frac{0.4}{0.7}}+1)^{-1} - 0.2\right) \approx 0.29$.

4. **(e)**: $\phi(3411) = \phi(3^2)\phi(379) = (3^2-3)378 = 2268$, so by Euler's Theorem,

$$5^{2272} \equiv 5^{2268} \times 5^4 \equiv 1 \times 625 \equiv 625 \pmod{3411}.$$

5. **(b)** For $n = 1113$, $\lceil\sqrt{n}\rceil = 34$, so

t	$2t+1$	$s^2 = t^2 - n$	$s \in \mathbb{Z}$?
34	69	43	×
35	71	112	×
36	73	183	×
37	75	256	✓

so $t = 37$ and $s = \sqrt{256} = 16$, and $a = t + s = 53$ and $b = t - s = 21$; hence, $1113 = n = ab = 53 \times 21$ and $a - b = 32$.

6. (i) **True**: Encode the message *bb•*:

	subinterval start	**width**
begin	0	1
b	0.3	0.4
b	$0.3 + 0.3 \times 0.4 = 0.42$	$0.4 \times 0.4 = 0.16$
•	$0.42 + 0.7 \times 0.16 = 0.532$	$0.16 \times 0.3 = 0.048$

so the message encodes as a number in the interval $[0.532, 0.58)$.

(ii) **False**: The binary entropy $H(S)$ is approximately 1.53 .

(iii) **False**: The second shortest codeword lengths are 4.

(iv) **True**: There are $\phi(125-1) = \phi(2^2)\phi(31) = 60$ primitive elements in GF(125).

(v) **False**: The pseudo-random numbers generated are 7, 2, 9, 6, 0, 5, 15, 1.

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

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

(ii) $\gamma, \gamma^3, \gamma^5, \gamma^7$

(iii) $\dfrac{\gamma^4 + \alpha}{\gamma^4 + \gamma} = \dfrac{2 + \alpha}{\alpha} = \dfrac{\gamma^7}{\gamma^6} = \gamma (= \alpha + 1)$

Version B

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

1. **(d)**: Encode the message $bb\bullet$:

	subinterval start	width
begin	0	1
a	0	0.5
b	$0.5 \times 0.5 = 0.25$	$0.4 \times 0.5 = 0.2$
$\bullet$	$0.25 + 0.9 \times 0.2 = 0.43$	$0.1 \times 0.02 = 0.45$

   so the message encodes as a number in the interval $[0.43, 0.45)$.

2. **(a)**: $H_M = \frac{3}{5}H(0.7) + \frac{2}{5}H(0.4) \approx 0.917$

3. **(a)**: $I(A,B) = H(B) - H(B|A) = H(0.3 + 0.7p) - (0.5p + 0.1)$,
   so $\frac{d}{dp}I(A,B) = 0.7\log_2(\frac{1}{0.3+0.7p} - 1) - 0.5$.
   Setting $\frac{d}{dp}I(A,B) = 0$ yields $p = \frac{1}{0.7}\left((2^{\frac{0.5}{0.7}} + 1)^{-1} - 0.3\right) \approx 0.11$.

4. **(d)** For $n = 1215$, $\lceil\sqrt{n}\rceil = 35$, so

t	$2t+1$	$s^2 = t^2 - n$	$s \in \mathbb{Z}$?
35	71	10	×
36	73	81	✓

   so $t = 36$ and $s = \sqrt{81} = 9$, and $a = t + s = 45$ and $b = t - s = 27$;
   hence, $1215 = n = ab = 45 \times 27$ and $a - b = 18$.

5. **(e)**: $\phi(99) = \phi(3^2)\phi(11) = 6 \times 10 = 60$, so by Euler's Theorem,
$$5^{66} = 5^{60} \times 5^6 \equiv 1^{60} \times (5^3)^2 \equiv 125^2 \equiv 26^2 \equiv 676 \equiv 82 \pmod{99}.$$

6. (i) **False**: 1. a, 2. b, 3. ba, 4. bb, 5. bba
   (ii) **True**: The ternary entropy is approximately 0.817.
   (iii) **True**: $\gcd(8, 65) = 1$ and $8^{64} \equiv 1 \pmod{65}$.
   (iv) **True**: Codeword lengths: 1, 3, 3, 4; codewords: 0, 100, 101, 1100.
   (v) **True**: $20 \equiv 5^5 \mod 23$ and $\gcd(5, 22) = 1$.

7. (i) Here, we have that $\alpha^3 = \alpha + 1$.

$$\begin{array}{|ll|}\hline \alpha^1 & = \alpha \\ \alpha^2 & = \alpha^2 \\ \alpha^3 & = \alpha + 1 \\ \alpha^4 & = \alpha^2 + \alpha \\ \alpha^5 & = \alpha^2 + \alpha + 1 \\ \alpha^6 & = \alpha^2 + 1 \\ \alpha^7 & = 1 \\ \hline \end{array}$$

   (ii) $\alpha^{3k} = (\alpha + 1)^k = \alpha^2 + \alpha + 1 = \alpha^5 = \alpha^{12}$, so $3k \equiv 12 \pmod 7$; hence, $k = 4$.
   (iii) $\{\alpha^6, \alpha^{12} = \alpha^5, \alpha^{10} = \alpha^3, \alpha^6 \ldots\} = \{\alpha^3, \alpha^5, \alpha^6\}$,
   so the minimal polynomial of α^3 is

$$\begin{aligned} &(x - \alpha^3)(x - \alpha^5)(x - \alpha^6) \\ &= x^3 - (\alpha^3 + \alpha^5 + \alpha^6)x^2 + (\alpha^3\alpha^5 + \alpha^3\alpha^6 + \alpha^5\alpha^6)x - \alpha^3\alpha^5\alpha^6 \\ &= x^3 + (\alpha + 1 + \alpha^2 + \alpha + 1 + \alpha^2 + 1)x^2 + (\alpha + \alpha^2 + \alpha^4)x + 1 \\ &= x^3 + x^2 + (\alpha + \alpha^2 + \alpha^2 + \alpha)x + 1 \\ &= x^3 + x^2 + 1\,. \end{aligned}$$